



*Router*

*Command Line Interface*

*Reference Manual*

*For DI-1750/DI-2630/DI-3660*

---

---

Rev. 1 (Jan 2003)

---



RECYCLABLE

## Software Configuration Guide of Router

1. Prepare for Configuration .....	11
1.1 Preparation .....	11
1.2 Port Number .....	11
1.3 Before Start .....	12
1.4 Get Help .....	12
1.5 Command Directory .....	12
1.6 Cancel A Command .....	12
1.7 Saving Configuration .....	13
2. Configure System Monitor Status .....	14
2.1 File System Commands .....	14
2.2 File System Command .....	14
2.2.1 Update Software .....	14
2.2.2 Update Configuration .....	15
2.3 Configure Ethernet IP Address .....	16
2.4 Configure The Default Route .....	16
2.5 Test Network Connection By PING .....	16
2.6 Manually Boot From A File .....	16
3. Interface Configuration .....	17
3.1 Overview .....	17
3.2 Introduction of Interface Configuration .....	18
3.3 Introduction of Sub-interface .....	19
3.4 Configure public configuration of interface .....	19
3.4.1 Set bandwidth .....	20
3.4.2 Set timing delay .....	20
3.4.3 Adjust Maximum Packet Unit(MTU) Size .....	20
3.5 Initialize and delete interface .....	22
3.6 Close and restart interface .....	22
3.7 Configuring Interface .....	23
3.7.1 Configuring Ethernet Interface .....	23
3.7.2 Configure the rate of FastEthernet .....	24
3.7.3 Duplex configuration mode of FastEthernet .....	25
3.7.4 Configuring Synchronous Serial Interface .....	26
3.8 Configuring E1 interface .....	28
3.9 Configure the BRI interface .....	33
3.10 Configure DTU interface .....	33
3.11 configuring the MODEM interface .....	34
3.12 Configuring SNMP List .....	40
3.13 configuring the CDP .....	45
3.14 Directory of VTY configuration .....	48
4. WANs Configuration .....	59
4.1 Overview .....	59
4.1.1 Destination of File .....	59
4.1.2 Frame Relay (FR) .....	59
4.1.3 LAPB and X.25 .....	60
4.1.4 HDLC .....	60
4.1.5 SLIP .....	60
4.1.6 PPP .....	61
4.2 Frame Relay Configuration Task List .....	61

4.2.1	Configuring Frame Relay .....	61
4.2.2	Frame Relay Hardware Configurations .....	61
4.2.3	Frame Relay Configuration Task .....	62
4.2.4	Enable Frame Relay Encapsulation on interface .....	62
4.2.5	Configuring Dynamic or Static Address Mapping .....	63
4.2.6	Configure Dynamic Mapping .....	63
4.2.7	Configure Static Mapping .....	63
4.2.8	Straight configure the LMI .....	64
4.2.9	Set the LMI Type .....	64
4.2.10	Set the Polling Intervals and Timer .....	65
4.2.11	Configure Frame Relay Switching .....	66
4.2.12	Configure a Frame Relay supported DTE Device, DCE Switch, or NNI interface .....	66
4.2.13	Specify the Static Route .....	67
4.2.14	Disable or Reenable Frame Relay Inverse ARP .....	68
4.2.15	Configure Frame Relay Subinterfaces .....	68
4.2.16	Understand Frame Relay Subinterfaces .....	68
4.2.17	Define Frame Relay Subinterfaces .....	69
4.2.18	Specify Subinterface Address .....	70
4.2.19	Configure DLCI .....	70
4.2.20	Configure Inverse ARP for Dynamic Address Mapping on Subinterfaces .....	71
4.2.21	Configure Static Address Mapping for Subinterfaces .....	71
4.2.22	Monitor and maintain the Frame Relay Connections .....	71
4.2.23	Frame Relay Configuration Examples .....	72
4.2.24	Encapsulation Examples .....	72
4.2.25	Static Address Mapping Examples .....	72
4.2.26	Frame Relay Switching Examples .....	72
4.2.27	PVC Switching Configuration Example .....	73
4.2.28	Pure Frame Relay DCE Example .....	73
4.2.29	Hybrid DTE/DCE PVC Switching Example .....	74
4.2.30	Subinterface Examples .....	75
4.3	X.25 Configuration Task List .....	76
4.3.1	Configure LAPB .....	76
4.3.2	Set default flow control values .....	81
4.3.3	Set the X.25 level 3 timers .....	82
4.3.4	Set the X.25 address .....	82
4.3.5	Mapping protocol addresses to X.121 addresses .....	83
4.3.6	set the encapsulation for virtue circuit idle time .....	86
4.3.7	Configure the X.25-TCP switching parameters .....	87
4.3.8	configure PVC switching between X.25 interfaces .....	88
4.3.9	Configuring the virtue circuit ranges .....	97
4.4	Configuring X.25 PAD Operation Task List .....	99
4.4.1	Network Topology .....	99
4.4.2	About Network Topology .....	99
4.4.3	Configuration Task List .....	100
4.4.4	Place and Clear Calls .....	101
4.4.5	Place a Call .....	101
4.4.6	Clear a Call .....	102
4.4.7	Customerize Local X.3 Parameter .....	102
4.4.8	Monitor X.25 PAD Connection .....	103

4.4.9	PAD Signal Examples .....	104
4.4.10	X.3 Customization Examples .....	104
4.4.11	X.3 Profile Example .....	105
4.4.12	Getting Help Example .....	105
4.4.13	Monitoring X.25 Network Example .....	105
4.5	Configuring PPP Task List .....	105
4.5.1	Implementation Information .....	106
4.5.2	PPP Configuration Task List .....	106
4.5.3	Enabling PPP Encapsulation .....	106
4.5.4	Enabling CHAP or PAP Authentication .....	107
4.5.5	Start Callback Control Protocol(CBCP) .....	109
4.5.6	Configuring IP Address Pool .....	112
4.5.7	Peer Address Allocation .....	112
4.5.8	Precedence Rules .....	112
4.5.9	Interfaces Affected .....	112
4.5.10	Configuring IP Address Assignment for each Interface .....	112
4.5.11	Disabling or Reenabling Peer Host Routes .....	115
4.5.12	Configuring Multilink PPP .....	115
4.5.13	Configuring Multilink PPP on Dialing Line .....	116
4.5.14	Configuring MLP on a Single ISDN BRI Interface .....	119
4.5.15	Configuring MLP on Multiple ISDN BRI Interfaces .....	123
4.5.16	Configure Multilink PPP on DSL .....	129
4.5.17	PPP Configuration Example .....	132
4.5.18	CHAP Configuration Example .....	133
4.5.19	Multilink PPP Configuration Example .....	133
4.5.20	PPPoE Client Illustration .....	135
4.5.21	PPPoE Client Configuration Example .....	135
4.6	Configuring SLIP Task List .....	136
4.6.1	Implementation Information .....	136
4.6.2	SLIP Configuration Task List .....	136
4.6.3	Enable SLIP Encapsulation .....	137
4.7	Configuring HDLC Task List .....	137
4.7.1	Implementation Information .....	137
4.7.2	HDLC Confiureation Task List .....	137
4.7.3	Enable HDLC Encapsulation .....	137
4.8	Configuring ISDN BRI Task List .....	138
4.8.1	ISDN BRI Interface Configuration Task List .....	139
4.8.2	ISDN BRI Interface Configuration Examples .....	139
5.	IP section of network protocol configuration .....	146
5.1	IP Overview .....	146
5.1.1	IP Routing Protocol .....	146
5.1.2	Select a routing protocol .....	146
5.1.3	Interior Gateway Protocols .....	146
5.1.4	Exterior Gateway Protocols .....	147
5.2	Configure IP Addressing .....	147
5.2.1	IP Addressing Task List .....	147
5.2.2	Assign an IP Addresses to a Network Interface .....	147
5.2.3	Assign Multiple IP Addresses to a Network Interface .....	148
5.2.4	Enable IP Processing on a Serial Interface .....	149

5.2.5 Configure Address Resolution .....	150
5.3 Configuring Network Address Translation (NAT) Task List .....	156
5.3.1 NAT Applications .....	156
5.3.2 Benefits of NAT .....	156
5.3.3 NAT Terminology .....	157
5.3.4 NAT Configuration Task List .....	157
5.3.5 Translating Inside Source Addresses .....	157
5.3.6 Configuring Static Translation .....	158
5.3.7 Configuring Dynamic Translation .....	160
5.3.8 Overloading an Inside Global Address .....	163
5.3.9 Translating Overlapping Addresses .....	168
5.3.10 Configuring Static Translation .....	168
5.3.11 Configuring Dynamic Translation .....	170
5.3.12 Providing TCP Load Distribution .....	174
5.3.13 Changing Translation Timeout and Restrict Connection Amount .....	178
5.3.14 Monitoring and Maintaining NAT .....	181
5.3.15 NAT Configuration Examples .....	182
5.4 Configure DHCP Client .....	184
5.4.1 DHCP Applications .....	184
5.4.2 DHCP Benefits .....	184
5.4.3 DHCP Terms .....	184
5.4.4 DHCP Client Configuration Task List .....	185
5.4.5 Obtain an IP for an Ethernet Interface .....	185
5.4.6 Specify DHCP-Server .....	185
5.4.7 Configure DHCP Parameters .....	186
5.4.8 Obtain an IP from DHCP-Server for PPP Interaction .....	186
5.4.9 Monitor DHCP .....	187
5.4.10 DHCP Client Configure Example .....	187
5.5 Configure IP Service Task List .....	193
5.5.1 IP Service Task List .....	193
5.5.2 Manage IP Connection .....	194
5.5.3 Configure IP over WANs .....	200
5.6 Filter IP Packets Task List .....	203
5.6.1 Filter IP Packets .....	203
5.6.2 Create Standard and Extended Access Lists .....	204
5.6.3 Apply the Access List to an Interface .....	206
5.6.4 Extended Access List Examples .....	207
5.7 Configure RIP Task List .....	208
5.7.1 Configure RIP .....	208
5.7.2 RIP Configuration Task List .....	208
5.7.3 Enable RIP .....	208
5.7.4 Allow Unicast Updates for RIP .....	210
5.7.5 Apply Offsets to Routing Metrics .....	211
5.7.6 Adjust Timers .....	211
5.7.7 Specify a RIP Version .....	212
5.7.8 Enable RIP Authentication .....	213
5.7.9 Disable Route Summarization .....	215
5.7.10 Disable the Validation of Source IP Addresses .....	215
5.7.11 Enable or Disable Split Horizon .....	215

5.7.12 Monitor and Maintain RIP .....	216
5.7.13 RIP Configuration Examples .....	217
5.8 Configure BEIGRP Dynamic Route Protocol .....	217
5.8.1 Brief Introduction of BEIGRP Route Protocol .....	217
5.8.2 BEIGRP Configuration Task List .....	218
5.8.3 Enable BEIGRP .....	218
5.8.4 Configure the Percentage of Link Bandwidth Used .....	220
5.8.5 Adjusting the BEIGRP Calculating Coefficient of Metrics .....	222
5.8.6 Apply offset to Adjust Routing Metrics .....	223
5.8.7 Disabling Route Automatic Summarization .....	224
5.8.8 Customize Route Summary .....	224
5.8.9 Configure Other BEIGRP Parameters .....	226
5.8.10 Adjusting the BEIGRP Send Hello Packets Interval and Neighbor Out-time .....	226
5.8.11 Disabling Horizontal Split .....	229
5.8.12 Monitor and Maintain BEIGRP .....	229
5.8.13 BEIGRP Configuration Example .....	235
5.9 Configuring OSPF Task List .....	235
5.9.1 Configuring OSPF .....	235
5.9.2 The D-Link Router OSPF Implementation .....	235
5.9.3 OSPF Configuration Task List .....	235
5.9.4 Enabling OSPF .....	236
5.9.5 Configuring OSPF Interface Parameters .....	237
5.9.6 Configuring OSPF over Different Physical Networks .....	238
5.9.7 Configuring Your OSPF Network Type .....	238
5.9.8 Configuring Point-to-Multipoint, Broadcast Networks .....	239
5.9.9 Configuring OSPF for Nonbroadcast Networks .....	241
5.9.10 Configuring OSPF Area Parameters .....	244
5.9.11 Configuring Route Summarization In OSPF Area .....	245
5.9.12 Configuring Route Summarization When Redistributing Routes into OSPF .....	246
5.9.13 Generate a Default Route .....	246
5.9.14 Force the Router ID Choice with a Loopback Interface .....	247
5.9.15 Configure the OSPF Administrative Distances .....	248
5.9.16 Configure Route Calculation Timers .....	249
5.9.17 Monitor and Maintain OSPF .....	249
5.9.18 OSPF Configuration Examples .....	250
5.10 Configure BGP Task List .....	257
5.10.1 BGP Overview .....	257
5.10.2 D-Link BGP Implementation .....	257
5.10.3 Configure BGP Neighbors .....	260
5.10.4 Configure BGP Soft Reconfiguration .....	261
5.10.5 Reset BGP Connections .....	261
5.10.6 Configure synchronization between BGP and IGP .....	262
5.10.7 Configuring BGP Weights .....	263
5.10.8 Configure the BGP Route Filtering based on Neighbor .....	264
5.10.9 Configure the BGP Route Filtering based on Port .....	268
5.10.10 Disable Next-Hop Processing on BGP Updates .....	269
5.10.11 Configure Advanced BGP Features .....	269
5.10.12 Monitor and Maintain BGP .....	280
5.10.13 BGP Configuration Example .....	283

5.11 Configure RSVP .....	290
5.11.1 How to Enable RSVP on Router .....	290
5.11.2 How to Enable RSVP in IP Phone Module .....	291
5.11.3 Use RSVP Assistant Configuration Commands .....	291
5.11.4 How to Configure TOS and Precedence for RSVP Flow .....	292
5.11.5 How to Use access-list in RSVP module .....	293
6. Security Configuration .....	323
6.1 Configure AAA .....	323
6.1.1 AAA Overview .....	323
6.2 Configure RADIUS .....	339
6.2.1 RADIUS Overview .....	339
6.2.2 RADIUS Protocol Operation .....	340
6.2.3 RADIUS Configuration Steps .....	340
6.2.4 RADIUS Configuration Examples .....	343
6.3 Configure TACACS+ Directory .....	344
6.3.1 TACACS+ Overview .....	344
6.3.2 TACACS+ Protocol Operation .....	344
6.3.3 TACACS+ Configuration Process .....	345
6.3.4 TACACS+ Configuration Examples .....	348
6.4 Configure IPsec .....	350
6.4.1 About Configure IPsec .....	350
6.4.2 IPsec Overview .....	350
6.4.3 Overview of How IPsec Works .....	351
6.4.4 IPsec Configuration Steps .....	352
6.5 Configuring Internet Key Exchange Security Protocol .....	366
6.5.1 Overview .....	366
6.5.2 About IKE .....	366
6.5.4 IKE Configuration Steps .....	367
6.5.5 What To Do Next .....	374
6.5.6 IKE Configuration Examples .....	374
7. QoS Configuration .....	376
7.1 QoS Overview .....	376
7.1.1 What is QoS .....	376
7.1.2 End-to-End QoS Models .....	376
7.1.3 QoS Queueing Algorithms .....	377
7.1.4 QoS Signalling .....	379
7.1.5 QoS Link Efficiency Mechanisms .....	379
7.2 Configure QoS .....	379
7.2.1 QoS Queueing Configuration .....	379
7.2.2 QoS Display .....	395
7.2.3 QoS Configuration Project .....	400
7.3 Configure RTP Header Compression Protocol .....	401
7.3.1 CRT Configuration Steps .....	401
7.3.2 Brief Introduction Of CRTP .....	401
7.3.3 Enable CRTP On A Serial Interface .....	402
7.3.4 Display CRTP Compression Information .....	405
7.3.5 CRTP Debugging .....	406
7.3.6 Configuration Examples .....	408
7.4 Configure CTCP (TCP/IP Header-Compression Protocol) .....	408

7.4.1 CTCP Configuration Steps .....	408
7.4.2 About CTCP .....	408
7.4.3 Enable CTCP On A Serial Line .....	409
7.4.4 Change The Maximum Number Of CTCP Connections .....	411
7.4.5 Display CTCP Compression Information .....	412
7.4.6 CTCP Debugging .....	414
7.4.7 Configuration Example .....	415
8. Dialer Configuration .....	415
8.1 About dialer .....	415
8.2 Software Configuration of Dialer .....	415
8.3 Dialer Configuration Tasks .....	415
8.4 DDR configuration command list .....	415
8.5 Configuring an Interface to Send and Receive calling .....	416
8.6 Customize the DDR Network .....	424
8.7 Monitoring and Maintaining the Dialer Connection .....	429
8.8 Dailer Configuration Example .....	430
8.8.1 The example of dialing to Multiple points .....	430
8.8.2 Configuring Dialer Rotary Groups Example .....	430
8.8.3 The examples of dialing to one or multiple points with dialer map .....	431
8.9 Script Configuration Example .....	431
8.9.1 Modem Script Execution Example .....	431
8.9.2 Login Script Execution Example .....	432
8.10 launch flow equilibrium backup .....	436
8.11 interface backup configuration example .....	438
9. IP Voice Configuration Task List .....	441
9.1 About Voice .....	441
9.2 About Voice Application .....	441
9.3 Dial Peers .....	441
9.4 Voice Port .....	442
9.5 Voice Primer .....	442
9.6 Numbering Scheme .....	442
9.7 Analog versus Digital .....	442
9.8 CODECs .....	443
9.9 Mean Opinion Score .....	443
9.10 Delay .....	444
9.11 Jitter .....	444
9.12 End-to-end Delay .....	444
9.13 Echo .....	444
9.14 About QoS .....	445
9.14.1 What is QoS .....	445
9.14.2 End-to-End QoS Module .....	445
9.14.3 Best-Effort Service .....	445
9.14.4 Integrated Service .....	445
9.14.5 Differentiated Service .....	445
9.15 QoS Signalling .....	445
9.15.1 Configure Voice over IP .....	447
9.15.2 How Voice over IP Processes a Telephone Call .....	447
9.15.3 Prerequisite Tasks .....	447
9.15.4 Voice over IP Configuration Task List .....	448

9.15.5 Configure Dial Peers .....	448
9.15.6 Create a Dial Peer Configuration Table .....	450
9.15.7 Configure POTS Dial Peers .....	450
9.15.8 Configure VoIP Dial Peers .....	451
9.16 Validation Tips .....	452
9.17 Troubleshooting Tips .....	452
9.17.1 Voice over IP Configuration Examples .....	454
9.17.2 FXS-to-FXS Connection .....	454
9.17.3 PSTN Gateway Access Using FXO Connection .....	455
9.18 Configure dial flow .....	465
9.18.1 Configuration in IVR dial-peer .....	465
9.18.2 Configure authentication information .....	466
9.18.3 Configure dial information .....	466
9.18.4 Configuration in IVR dial-peer .....	467
9.18.5 Configuration in IVR dial-peer .....	468
9.17 Configure record file name .....	468
9.18.6 Configure the default recording time .....	468
10. IBM Networking Configuration .....	474
10.1 Configure DLSW Task List .....	474
10.1.1 Configure DLSW .....	474
10.1.2 How to use DLSw Configuration Commands .....	474
10.1.3 How to use the function of showing DLSw .....	475
10.1.4 How to use the DLSw 's Debug Function .....	476
10.1.5 How to use the DLSw Management Function .....	476
10.2 Configuring LLC2 .....	476
10.2.1 Configure the DLSw idle-time .....	476
10.2.2 Configure the wait-for-response time .....	477
10.2.3 Configure the remote-busy time .....	478
10.2.4 Configure the response time .....	479
10.2.5 Configure the reject-time .....	479
10.2.6 Configure the LLC2 window size .....	480
10.2.7 Configure the holdqueue packet-count .....	481
10.2.8 Configure the ack-delay times(seconds) .....	482
10.2.9 Configure the ack-max number .....	482
10.2.10 Show LLC2 link information .....	482
10.2.11 Debug the LLC2 link information .....	483
10.3 SDLC Configuration Task List .....	485
10.3.1 Configure the Router as SDLC Primary or Secondary Station .....	485
10.3.2 Establishing an SDLC Station for DLSW+ Support .....	485
10.3.3 Set the SDLC as Two-way Simultaneous Mode .....	486
10.3.4 Configure SDLC Timer and Retry Counts .....	487
10.3.5 Configure the Amount of SDLC Frames and Information Frames .....	487
10.3.6 Control the Buffer Size .....	488
10.3.7 Control Polling of Secondary Stations .....	489
10.3.8 Configure an SDLC Interface for Half-Duplex Mode .....	489
11 VPDN configuration task list .....	494
11.1 VPDN module encapsulation .....	494
11.2 create VPDN group .....	494
11.3 set VPDN group as LNS dial mode .....	494

---

11.4 set LAC domain name .....	496
11.5 set remote LNS connected with LAC ip address .....	496
11.6 set VPDN group local tunnel name .....	497
11.7 set remote LAC tunnel name connected with LNS .....	497
11.8 reconfirm LNS and CLIENT .....	498
11.9 LCP renegotiate LNS and CLIENT .....	498
11.10 set VPDN group source IP address .....	499
11.11 clone configured source interface on LNS workgroup .....	499
11.12 tunnel authentication .....	499
11.14 set tunnel password .....	500
11.15 set time interval of sending HELLO diagram .....	501
11.16 set tunnel accepting window size .....	501
11.17 set L2TP property hidden .....	502
11.18 display VPDN group .....	502
11.19 display L2TP event information .....	503
11.20 display L2TP packet information .....	504
11.21 display the mistake during L2TP transferring .....	504
11.22 configuration example .....	505

## 1. Prepare for Configuration

### 1.1 Preparation

In this section, we will introduce the necessary information for the first time configuration of Router, which includes port numbering, introduction of operation and command line interface before start.

### 1.2 Port Number

- ◆ The number of the Router's physical port is in the form of <type><slot>/<port>, following is the relation table of the type and it's name.

Type Of Interface	Name Of Type	Shortened Form
Serial Port	Serial	s
Synchronous Port	Serial	s
Asynchronous Port/Aux	Async	a
10M Ethernet	Ethernet	e
100M Fast Ethernet	Fast Ethernet	f
ISDN BRI	BRI	b
E1(ISDN PRI)	Serial	s

- ◆ The values of slots have fixed numbers for the WIC/VIC extended slot. The method is that the right to left numbering for horizontal and up to down for vertical. Zero is the fixed value as standard configuration. The others values are numbered according to sequence above and start from 1 even network extended slot or voice extended slot.
- ◆ The values of port are wholly numbered form right to left and start from 0. If there's only one port, it will be tagged as 0.
- ◆ According to the rules above, the number for each series of product is listed as follows:

Product Model	Configuration	Number
DI-1750	Standard Config 10\100M Ethernet Interface	FastEthernet0/0
	Standard Config Aux Interface	Async0/0
	Interface Card Slot	From right to left in turn is slot1~2 Network/Voice Interface Slot :slot1&slot2
DI-2630	Interface Card Slot	From right to left in turn is slot1~2
	Standard Config 10\100M Ethernet Interface	FastEthernet0/0
	Standard Config Aux Interface	Async0/0
DI-3660	Standard Config Aux Interface	Async0/0
	Interface Card Slot	There are 3 rows of slots , the lowest row is slot1~2(from right to left) ; the middle is slot3~4(from right to left) ; the above row is slot5~6(from right to left).

*Notice:*

Please number the combination cards and modules in the sequence of from right to left; For the supported types of NM ,

WIC , FIC slot modules or interface cards, please refer to Hardware Description.

### 1.3 Before Start

Please confirm the following steps before power on the router for configuration:

Step 1. Set up Router's hardware according to the requirement of User Manual

Step 2. Configure the PC terminal emulation program

Step 3. For Internet Protocol (IP), decide:

- Layout of IP addresses
- Which WAN (Wide Area Network) protocols (egg. Frame Relay, HDLC、X.25) are to be used on each port

### 1.4 Get Help

ls command and its -l option can help to input the commands:

- Type in ls command to display the list of currently available commands

```
[DEFAULT@Router /]#ls
```

- Type in ls -l command to display the list of currently available commands and the brief introduction

```
[DEFAULT@Router /]#ls -l
```

- Press Up direction key to display the formerly input commands. To display more commands please continue to press the Up key.

### 1.5 Command Directory

The Router user interface includes various directories, each of them enable you to configure different components on the Router. The currently available command relies on the location of your command directory. Type in the ls command to display the available command list under each command directory. The following table lists the frequently used commands:

Command Directory	Entry Method	Interface Promote	Quit Method
System Monitor Directory	Power on the device and input ""Ctrl+Break	monitor#	By <i>quit</i> command
User Directory	Log in	[DEFAULT@Router/]#	By <i>exit</i> or <i>quit</i> command
Management Directory	Input "cd enable" command under the User Directory	[DEFAULT@Router#enable/]#	By <i>cd..</i> command
Global Configuration Directory	Input "cd config" command under the Management Directory	[DEFAULT@Router/config/]#	Use <i>cd..</i> command to return to the Management Directory

Each command directory has a limit to use the subset of commands. If you have a problem when inputting the command, please check the prompt and input ls command to obtain available commands list.

Please notify the new command directory that displayed by the change of interface prompt in the following example :

```
[DEFAULT@Router/]# cd enable
```

```
Password: <enter password>
```

```
[DEFAULT@Router/enable/]# cd config
```

```
[DEFAULT@Router/config/]# cd ..
```

```
[DEFAULT@Router/enable/]# cd ..
```

```
[DEFAULT@Router/]#
```

### 1.6 Cancel A Command

If you want to cancel a command or restore it to default properties, you can select U or u option at prompt rightly after inputting most of the commands.

For example, when deleting a configured static route, please select the U option at prompt after inputting the ip command, and then select route option, finally, input the parameter values of the route that you are about to delete.

### 1.7 Saving Configuration

You may need to save the configuration changes, so that you can quickly restore the original configuration in case of the system rebooting or power off failure. Write command can be used for saving the configuration under the Management or Global Configuration Directory.

## 2. Configure System Monitor Status

The following message will be displayed when switch on the Router (take DI-1750 for example):

```
D-Link Internetwork Operating System Software
1750 Series Software, Version 1.3.1D (FULL), RELEASE SOFTWARE
Copyright (c) 2002 D-Link Corporation.
Compiled: 2003-6-5 10:50:53 by HYZHU, Image text-base: 0x6004
ROM: System Bootstrap, Version 0.2.3
Serial num:D30113100040, ID num:002430
System image file is "0605.bin"
Please wait system check ram.....
```

At this time, please type in "aaa" to enter the System Monitor Status. The following display

Check ram OK

Welcome to D-Link Multi-Protocol 1700 Router

monitor#

Indicates the successful entry to the System Monitor Status.

Notice:

Since the System Monitor Status is with the highest authority, the incorrect operation may cause system Breakdown. Therefore, only the terminal connected to the console port is allowed to enter this status.

The user can handle the following tasks under the system monitor status:

- 1 . Management of file system, including *add* and *delete* a file. Since the router software and configuration is saved as file forms, the user can update or delete the software and the configuration.
- 2 . Configure Ethernet IP addresses.
- 3 . Test the network connection by PING test.
- 4 . Start from a file manually.

The following is usage of the commands in detail under the system monitor status.

### 2.1 File System Commands

There are only as most as 20 characters in a FLASH file name, and not case-sensitive.

### 2.2 File System Command

The boldface parts of all commands are the key words, the others are parameters. The parts inside the [] are optional settings.

#### ◆ **Format**

Format the file system and delete all data.

#### ◆ **dir** [file name]

Display the file name and directory. The file name in [ ] displays a file that begins with certain letters. The displayed form is as follows:

```
Index number file name <FILE> file length creation time
```

#### ◆ **delete** filename

Delete a file. It will be prompted if the file to be deleted does not exist.

#### 2.2.1 Update Software

This command is used to download the router system software from local or remote sites, for the version update or customized version with special functions (eg. data encryption).

There are two methods to update the software in the monitor status.

#### **A . By TFTP Protocol**

```
monitor#copy tftp<:filename> flash <:filename> [ip_addr]
```

This command is used to copy the file from tftp server to system flash memory. The system will prompt user to input the

name of remote server and remote file upon typing the command.

**Parameter Description**

tftp<:filename> Indicates reading the files from the tftp server. “Filename” will indicate the relative filename, if not, the user will be prompted to input the filename after the “copy” command operates.

flash<:filename> Indicates writing a file into the router flash. The filename will indicate the relative filename, if not, the user will be prompted to input the filename after the “copy” command operates.

ip\_addr The IP address of tftp server. If it is not specified, the user will be prompted to input the filename after the “copy” command operates.

**Example**

Read the file named “main.bin” in the TFTP server and write it into Router as “router.bin”

```
monitor#copy tftp flash:router.bin
```

```
Prompt: Remote-server ip address[?]192.168.0.116
```

```
Prompt: Name of remote file to read[?]main.bin
```

```
TFTP:successfully receive 36 blocks ,18370 bytes
```

```
monitor#
```

**B . By SLIP zmodem**

Update the software with “download” command. Input “download ?” to obtain help.

```
monitor#download c0 <local_filename>
```

This command is used to copy a file to the system flash memory through SLIP zmodem. The system will prompt to input the port rate upon inputting the command.

**Parameter Description**

local\_filename A file name stored in the flash memory. The user must input the filename.

**Example**

The terminal program can use the Hyper Terminal program of WINDOWS 95 , NT 4.0 or terminal emulation program of WINDOWS 3.X.

```
monitor#download c0 router.bin
```

```
Prompt: speed[9600]?115200
```

Then modify the rate to 115200. After reconnection, select Send File in the Send menu of a hyper terminal (terminal emulation), as the following graph:

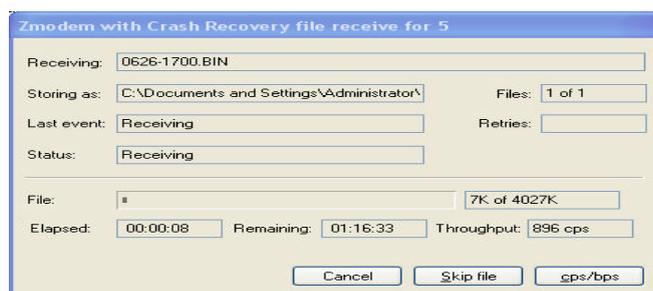


Fig. 2-3-1

Input the full path of Router software main.bin provided by this company in the filename input box, and choose Zmodem for the protocol. Press “Send” button to send the file.

When completing sending the file, the following message will appear:

```
ZMODEM:successfully receive 36 blocks ,18370 bytes
```

```
monitor#
```

That means the successful update of the software.

**2.2.2 Update Configuration**

The Router configuration is saved as a file, named startup-config, which can be updated by a command that resembles the software update command.

**A . By TFTP protocol**

```
monitor#copy tftp flash:startup-config
```

### B . By SLIP zmodem.

```
monitor#download c0 flash:startup-config
```

## 2.3 Configure Ethernet IP Address

```
monitor#ip address <ip_addr> <net_mask>
```

This command is to configure the Ethernet IP address. The system default is 192.168.0.1, subnet mask 255.255.255.0.

### Parameter Description

ip_addr	Ethernet IP address
net_mask	Ethernet network mask

### Example

```
monitor#ip address 192.168.1.1 255.255.255.0
```

## 2.4 Configure The Default Route

```
monitor#ip route default <ip_addr>
```

This command is to configure the default route, and can configure only one route.

### Parameter Description

ip_addr	IP Address of the Gateway
---------	---------------------------

### Example

```
monitor#ip route default 192.168.1.1
```

## 2.5 Test Network Connection By PING

```
monitor#ping <ip_address>
```

This command is used for testing the connecting status of the network.

### Parameter Description

ip_address	Destination IP address
------------	------------------------

### Example

```
monitor#ping 192.168.0.100
Reply from 192.168.0.100 : data=48, time=10ms, ttl=128
4 packets sent, 4 packets received
round-trip min/avg/max = 0/2/10 ms
```

## 2.6 Manually Boot From A File

```
monitor#boot flash <local_filename>
```

This command is for starting some router software in the flash memory. There may be several router softwares in a flash.

### Parameter Description

local\_filename is the filename saved in the flash memory and must be input by user.

### Example

```
monitor#boot flash router.bin
```

### 3. Interface Configuration

#### 3.1 Overview

By the information in this chapter to understand the types of interfaces supported on D-Link routers and to search configuration information for various types of interfaces.

For a complete description of the interface commands used in this and other chapters that describe interface configuration, refer to the "[Interface Configuration Command](#)" chapter. To search documentation of other commands that appear in this chapter, please see the related contents of user manual.

This chapter contains general information that applies to all interface types; it includes these sections:

#### Supported types of interface

Please see the following form to obtain correlative information about the type of interface.

Types of Interface	Task	Reference information
LAN interface	<ul style="list-style-type: none"> <li>• Configure Ethernet interface</li> <li>• Configure FastEthernet interface</li> </ul>	<a href="#">“Configure LAN interface”</a>
Serial interface	<ul style="list-style-type: none"> <li>• Configure Synchronous Serial interface</li> <li>• Configure low-speed Serial interface</li> </ul>	<a href="#">“Configure Serial interface”</a>
Logic interface	<ul style="list-style-type: none"> <li>• Configure Loop-back interface</li> <li>• Configure Empty interface</li> <li>• Configure Dialup interface</li> <li>• Virtual template and virtual access interface</li> <li>• Multi-link interface</li> <li>• Tunnel interface</li> <li>• Sub-interface</li> </ul>	<a href="#">“Configure Logic interface”</a>
E1 interface	<ul style="list-style-type: none"> <li>• Configure channelized E1 interface</li> </ul>	<a href="#">“Configure E1 interface”</a>
PRI interface	<ul style="list-style-type: none"> <li>• Configure PRI interface</li> </ul>	Configure PRI interface
BRI interface	<ul style="list-style-type: none"> <li>• Configure BRI interface</li> </ul>	<a href="#">Configure BRI interface</a>
DTU interface	<ul style="list-style-type: none"> <li>• Configure DTU interface</li> </ul>	<a href="#">Configure DTU interface</a>
MODEM interface	<ul style="list-style-type: none"> <li>• Configure the asynchronous MODEM interface</li> </ul>	<a href="#">Configure the MODEM interface</a>

- ◆ Two types of interfaces are supported by D-Link router: physical and virtual interfaces. The types of physical interfaces on a device depend on its standard communication interface and the interface module equipped on the router. The virtual interfaces that D-Link routers and access servers support include sub-interface and logic

interface. The sub-interface derived from physical interface. Please see [Introduction of sub-interface](#) for more details. The logic interface indicates the interface that created manually by user and without corresponding physical equipment.

Presently, the physical interfaces supported by D-Link Router that include:

- Ethernet
- FastEthernet
- Synchronous Serial
- Low-speed Serial
- Asynchronous Serial
- Channelized E1
- ISDN PRI interface
- ISDN BRI interface
- DTU interface
- Asynchronous MODEM interface

Presently, the logic interface supported by D-Link Router are:

- Loop-back interface
- Empty interface
- Dialup interface
- Virtual template and virtual access interface
- Tunnel interface
- Sub-interface

### 3.2 Introduction of Interface Configuration

These following instructions apply to all interface configuration processes. Users should begin interface configuration in global configuration mode and follow these steps:

1. Use the command “**interface**” to begin to configure the related interface parameters. User can use command “**show interface**” to display the interface. All the interfaces of the device will provide their status as follows:

```
[DEFAULT@4_2750 /enable/]#show
(00)alias                alias for command
.....
(19)interface            interface status and configuration
.....
```

Please Input the code of command to be excute(0-45): **19**

Input 17 , choose “ interface ” , it will prompt :

```
(00)FastEthernet        FastEthernet interface
(01)Ethernet            Ethernet interface
(02)Serial               Serial interface
(03)Async                Asynchronous interface
(04)Null                 Null interface
```

Please Input the code of command to be excute(0-4): **2**

Input 2 , choose “ Serial ” , the prompt will be :

Please input a interface name:**s1/0**

Input the value of type、 slot and port of the interface , it will display :

Serial 1/0 is administratively down, line protocol is down

Hardware is SCC Mode=Sync,Speed=64000

DTR=UP,DSR=DOWN,RTS=DOWN,CTS=DOWN,DCD=DOWN

MTU 1500 bytes, BW 64 kbit, DLY 20000 usec

Encapsulation HDLC, loopback not set

Keepalive set(10 sec)

If you want to configure the serial interface 1/0, input the following content:

```
[DEFAULT@router /config/]#interface
```

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

(08)Multilink Multilink-group interface

(09)Virtual-template Virtual template interface

(10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): **2**

Please input a interface name:s**1/0**

Will you excute it? (Y/N):**y**

In the interface configuration mode, it will wait for the user to input the “enter” string each time a configuration is performed. After input the “enter”, it will automatically display all the performable commands of the interface to provide to users.

---

**Notice:** It is not necessary to add a space between the interface type and interface number. For example, in the preceding line you can specify either serial 10/0 or serial 0/0. The command will work by either way.

---

2. The commands which define the protocols and applications to be implemented on the interface can be configured under the current interface configuration mode. All sort of commands will exist until quit the interface configuration mode or switch to another interface.

3. Once the configuration was completed, user is able to test the status of interface by the command **show** that list in the section “[Supervise and maintain interface](#)”.

---

**Notice:** Configuring channelized E1 interfaces requires additional steps. When you configure channelized T1 or channelized E1, you must first define the channels and the time slots that comprise the channels. Use the commands of “**controller E1**” and “**channel-group**”, and then use “**interface serial**” to configure generated serial interface.

### 3.3 Introduction of Sub-interface

Configuring multiple sub-interfaces on a single physical interface allows greater flexibility and connectivity on the network. A sub-interface is a mechanism that allows a single physical interface to support multiple logical interfaces or networks. That is, several logical interfaces or networks can be associated with a single hardware interface. Sub-interfaces are implemented in various WAN protocols, including Frame Relay and X.25 protocol.

### 3.4 Configure public configuration of interface

The following section describes commands that executed on any type of interface and thereby configure the common configuration of interface. The common configuration of interface that available to be configured includes:

- ◆ You can add a description about an interface to help you remember what is attached to it. This description is meant solely as a comment to help identify what the interface is being used for. The description will appear in the output of the following commands: ‘**show running-config**’, and ‘**show interfaces**’. To add a description for any interface, use the following command in interface configuration mode:

Command	Purpose
<b>description</b> <i>string</i>	Add description to current interface configuration

- ◆ Choose the item 9 of prompt and add the descriptions
- ◆ Please see the [“Example of interface description”](#) to get more examples of add description of interface.

### 3.4.1 Set bandwidth

The information of bandwidth is use to carry out the operational decision by upper layer protocol (ULP). Use following commands to set the bandwidth in the current interface:

Command	Purpose
<b>bandwidth</b> <i>kilobps</i>	Set the bandwidth for current configured interface

- \* Choose the item 1 of prompt and set the bandwidth
- \* The bandwidth is only a parameter of route that did not affect the communication rate of actual physical interface.

### 3.4.2 Set timing delay

The information of timing delay is used to carry out the operational decision by upper layer protocol (ULP). Following commands set the timing delay in the current interface:

Command	Purpose
<b>delay</b> <i>tensofmicroseconds</i>	Set the timing delay for current configured interface

- \* Choose the item 8 of prompt and set the delay
- The setting of timing delay is only set a parameter of information. This configuration command cannot adjust the actual timing delay of interface.

### 3.4.3 Adjust Maximum Packet Unit(MTU) Size

Each interface has a default maximum packet size or maximum transmission unit (MTU) size. This number generally defaults to 1500 bytes. On serial interfaces, the MTU size varies, but cannot be set smaller than 68 bytes. To adjust the maximum packet size, use the following command in interface configuration mode:

Command	Purpose
<b>Mtu</b> <i>bytes</i>	Set MTU for current configured interface

- \* Choose the item 20 of prompt and set the value of MTU

#### Supervise and maintain the interface

To supervise and maintain the interface by the tasks below:

#### Examine status of interface

D-Link Router supports the command that to display various information of interface, which is include the status of interface and version of hardware and software. Parts of interface supervising commands are listed in the form below.

Please see the “[Command of interface configuration](#)“ for details.

Use following commands:

Command	Purpose
<b>show interface</b> [type slot/port]	Display the status of interface
<b>show running-config</b>	Display current configuration
<b>show version</b>	Display setting of hardware, version of software, filename of configuring file, source image and boot image.

To display interface status, input the command “ show ” to list all the parameters in global configuration contents:

```
(00)alias                alias for command
.....
(19)interface           interface status and configuration
.....
```

Please Input the code of command to be excute(0-45): **19**

Input 19, choose the item “ interface ” and it will prompt:

```
(00)FastEthernet        FastEthernet interface
(01)Ethernet            Ethernet interface
(02)Serial              Serial interface
(03)Async               Asynchronous interface
(04)Null                Null interface
```

Please Input the code of command to be excute(0-4): <cr>

Input the value of type, slot and port of the interface to be displayed:

To display the current configuration, input the command “ **show** ” to list all the parameters in the global configuration contents:

```
(00)alias                alias for command
.....
(31)running-config      current configuration
.....
```

Please Input the code of command to be excute(0-45): **31**

Input 31,choose the item “ running-config ” , it will prompt :

```
(00)interface           interface current configuration
(01)<cr>
```

Please Input the code of command to be excute(0-1): **1**

Input 1, it will display all the current configurations.

To display the hardware configuration, software version, name, source and boot image of the configuration documents, input the command “**show**” in the global configuration contents:

```
(00)alias                alias for command
.....
(41)version             router version information
.....
```

Please Input the code of command to be excute(0-45): **41**

Input 41 , choose the item “ version ” , it will prompt :

```
(00)all                Show all module version information
```

(01)module Specify module

(02)<cr>

Please Input the code of command to be excute(0-2): **0**

Input 0 , choose the item “ all ” , it will display all the information:

### 3.5 Initialize and delete interface

The logical interface can be created and dynamic deleted by user. The sub-interface and channelized interface are also can be dynamic deleted. Restore the default setting is available for the physical interface that cannot be dynamic deleted.

Following commands apply to initialize and delete the interface in the global configuration mode:

Command	Purpose
<b>Interface(undo) type slot/port</b>	Initialize physical interface or delete virtual interface

Input the command “ **interface** ” , it will list all the parameters :

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10): **u**

Input U or u, the prompt is :

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10):

Input the type, slot and port of the physical interface to be initialized or the virtual interface to be deleted.

### 3.6 Close and restart interface

Forbid an interface will cause the forbiddance of all the functions that use to assigned interface. Furthermore, the forbidden interface will be display as unavailable interface for all the supervising commands. This message will be transfer to other Routers through dynamic route protocol. Modify of any route will not effect the interface. Stop an interface on the serial interface will cause the reduction of DTR signal.

Use following command to close interface in the configuring mode of interface and then restart:

Step	Command	Purpose
1	<b>shutdown</b>	Stop interface
2	<b>Shutdown(default)</b>	Restart interface

Please use the commands show **interface** and **show running-config** to check an interface to be closed or not. In the command display of **show interface**, a closed interface will be displayed as “administratively down”. Please see the “[Example of stop interface](#)”.

#### Example of interface configuring

Provide following example of configuring process:

#### Example of start interface

Following example describe that how to start the interface configuring on a serial interface. It encapsulates PPP protocol

for serial interface 1/0.

```
interface serial 1/0
encapsulation ppp
```

**Example of interface description**

Following example explain that how to add the description of interface. The description will be presented with displaying of configuring file and interface command.

```
interface ethernet 1/1
description First Ethernet in network 1
ip address 192.168.1.23 255.255.255.0
```

**Example of stop interface**

Following example is of stop the Ethernet interface in port 1 of slot 1.

```
interface ethernet 1/1
shutdown
```

Following example is of restart interface

```
interface ethernet 1/1
shutdown(undo)
```

Following example is of stop an E1 channel

```
interface serial 1/3:23
shutdown
```

**3.7 Configuring Interface**

This chapter describes the processes for configuring interfaces. It contains these sections:

Please see the “Interface Configuration Example” later in this chapter to get the examples of configuring task. For hardware technical descriptions and information about installing interfaces, refer to the hardware installation and configuration manual for your product. For a complete description of the LAN interface commands used in this chapter, refer to the "Interface configuration commands" chapter.

**3.7.1 Configuring Ethernet Interface**

In this section, we will describe the process of Ethernet interface configuring. DLink Router supports the 10Mbps Ethernet interface and 100Mbps Fast Ethernet interface. The concrete configurations consist of following steps. The first step is prerequisite and others are optional.

◆ **Assign the interface of Ethernet or FastEthernet**

Input the commands below in global configuring mode to enter the status of Ethernet interface configuring

Command	Function
<b>interface ethernet</b> <i>slot/port</i>	Enter the mode of Ethernet interface configuring
<b>interface fastethernet</b> <i>slot/port</i>	Enter the mode of FastEthernet interface configuring

Input the command “ **interface** ” , it will list all the parameters:

```
(00)FastEthernet      FastEthernet interface
(01)Ethernet          Ethernet interface
(02)Serial            Serial interface
.....
```

Please Input the code of command to be excute(0-10): **1**

Input **1** , choose the item “ Ethernet ” , it will prompt :

Please input a interface name:

Input the Ethernet, slot and port name:

Input **0** , choose the item “ Fast Ethernet ” , it will display :

Please input a interface name:

Input the Fast Ethernet, slot and port name.

The command **show interface Ethernet** is use to display the status of Ethernet interface. The command **show interface fastethernet** is use to display the status of FastEthernet interface.

#### ◆ Configure 100Mbps FastEthernet

The FastEthernet interface of D-Link Router supports the rate of 10Mbps / 100Mbps and the Router, Hub and Switches with 100BaseT or 10BaseT interface. The FastEthernet interface support the adaptation with the rate of 10Mbps and 100Mbps. Furthermore, the FastEthernet is able to adopt the suitable rate of communication, which is according to the connected equipment. Following is the process of configuration that starts from management mode:

Step	Command	Function
1.	<b>cd configure</b>	Enter the content of global configuration
2.	<b>interface fastethernet slot/port</b>	Enter the FastEthernet interface
3.	<b>ip address address subnet-mask</b>	Set IP address and subnet mask on interface

Step 1:

Input the command “ cd config ” to enter the global configuration mode.

Step 2:

Input the command “ interface ” , list all the parameters:

```
(00)FastEthernet      FastEthernet interface
(01)Ethernet          Ethernet interface
(02)Serial            Serial interface
.....
```

Please Input the code of command to be excute(0-10): 0

Input 0 , choose the item “ fast Ethernet ” , it will prompt :

Please input a interface name:

Input the fast ethernet, slot and port name.

Step 3 :

Choose the item 20 of prompt, it will list all the parameters:

```
(00)access-group      Specify access control for packets
(01)address           IP address
(02)beigrp            Enhanced Interior Gateway Routing Protocol
.....
```

Please Input the code of command to be excute(0-19): 1

Input 1 , choose the item “ address ” , it will prompt :

```
(00)A.B.C.D          IP address
(01)dhcp             IP Address negotiated via DHCP
```

Please Input the code of command to be excute(0-1): 0

Input 0 , choose the item “ A.B.C.D ” , the prompt is :

Please input a IP Address:

Input the IP address, it will prompt :

Please input a IP Address:

Input the mask.

### 3.7.2 Configure the rate of FastEthernet

**The rate of FastEthernet executed through self-negotiation as well as configuration on interface.**

Command	Function
---------	----------

<b>Speed {10 100 auto}</b>	Set the rate of FastEthernet as 10M, 100M or self-negotiation.
<b>speed (default)</b>	Restore the default setting with the rate is self-negotiation.

Choose the item 35 of prompt, it will display that:

```
U(undo) D(default) Q(quit)
(00)10          Set 10-Mbps
(01)100        Set 100-Mbps
(02)auto       Set auto-speed
```

Please Input the code of command to be excute(0-2):

Input 0 to set the speed as 10M.  
 Input D or d, it will come back to default settings.

### 3.7.3 Duplex configuration mode of FastEthernet

**The duplex mode of FastEthernet executed through self-negotiation as well as configuration on interface.**

Command	Function
<b>duplex half</b>	Set the operational mode of FastEthernet as half-duplex.
<b>duplex full</b>	Set the operational mode of FastEthernet as full-duplex.
<b>Duplex(default)</b>	Restore the default setting as self-negotiation.

Choose the item 13 of prompt, it will display that:

```
U(undo) D(default) Q(quit)
(00)full      Force full duplex operation
(01)half      Force half duplex operation
```

Please Input the code of command to be excute(0-1):  
 Input 1, choose the item “half” can set it into half-duplex mode.  
 Input 0, choose the item “full” can set it into full-duplex mode.  
 Input D or d, it will come back to default settings.

◆ **Configure Ethernet subinterface**

This section is description about the process of Ethernet sub-interface configuring. D-Link Router supports the IEEE 802.1Q protocol on the Ethernet sub-interface. Detailed configuration as below:

◆ **Assign the sub-interface of Ethernet**

Input following commands under the global mode to enter the status of Ethernet interface configuring

Command	Function
<b>interface ethernet</b> <i>slot/port.subinterface-number</i>	Enter the status of Ethernet sub-interface configuring
<b>interface fastethernet</b> <i>slot/port.subinterface-number</i>	Enter the status of FastEthernet sub-interface configuring

Input the command “ interface ” , it will list all the parameters:

```
(00)FastEthernet      FastEthernet interface
(01)Ethernet          Ethernet interface
(02)Serial            Serial interface
.....
```

Please Input the code of command to be excute(0-10): **1**

Input 1, choose the item “ Ethernet ” , it will prompt:

Please input a interface name:

Input the name of Ethernet, slot and port and the value of sub-interface-number.

Input 0, choose the item “ Fast Ethernet ” , it will prompt:

Please input a interface name:

Input the name of Fast Ethernet, slot and port and the value of sub-interface-number.

#### ◆ Encapsulate 802.1Q protocol

**The sub-interface of Ethernet must encapsulate with 802.1Q protocol for usage. Otherwise, UP is unavailable for the protocol.**

Command	Function
<b>encapsulation dot1q</b> <i>vlan-identifier</i>	Encapsulate 802.1Q protocol and assign Vlan ID

Choose the item 11 of prompt, it will display:

(00)dot1Q            IEEE 802.1Q Virtual LAN

Please Input the code of command to be excute(0-0): **0**

Input 0 and the value of vlan-identifier , then the encapsulation of protocol for the sub-interface is complete.

#### Configuring Serial Interface

For hardware technical descriptions and information about installing interfaces, refer to the hardware installation and configuration publication for your product. For a complete description of serial interface commands used in this chapter, refer to the "Interface Command" chapter. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online, which is include following content:?

#### 3.7.4 Configuring Synchronous Serial Interface

The configuration of synchronous serial interface consists of following steps. The first step is prerequisite and others are optional.

Please see the "Example of interface configuring" in the last place to find the example of configuration task.

#### ◆ Specify Synchronous Serial Interface

In the global configuring mode, each following commands is use for assign the synchronous serial interface and enter the status of interface configuring (if asynchronous card be chose, e.g. 16 asynchronous card provides only asynchronous communication, use *async* to replace *serial*):

Command	Function
<b>interface serial</b> <i>slot/port</i>	Enter the interface configuring
<b>interface serial</b> <i>slot/port:set-channel-group</i>	Enter the channlized E1 interface configuring

Input the command “ **interface** ” and it will list all the parameters :

(00)FastEthernet            FastEthernet interface

(01)Ethernet                Ethernet interface

(02)Serial                    Serial interface

.....

Please Input the code of command to be excute(0-10): **2**

Input 2, choose the item “ serial ” , it will prompt:

Please input a interface name:

Input the serial, slot and port names, enter the interface configuration.

Input the name of the serial, slot, port and channel-group, enter the configuration of channelized E1 interface.

#### ◆ Specify Synchronous Serial Interface Encapsulation

By default, synchronous serial lines use the High-Level Data Link Control (HDLC) serial encapsulation method, which provides the synchronous framing and error detection functions of HDLC. The synchronous serial interfaces support the following serial encapsulation methods:

- High-level Data Link Control (HDLC)
- Frame Relay

- Point to point protocol (PPP)
- X.25
- Synchronous data link control ( SDLC )

The encapsulating protocol is able to set by following commands in the mode of interface configuring:

Command	Function
<b>encapsulation {hdlc frame-relay ppp x25 sdlc}</b>	Configure synchronous serial encapsulating protocol

The setting of concrete encapsulation should according to the actual situation. Please see the “[Command of interface](#)“ to get more information.

Choose the item 11 of prompt, it will list all the parameters:

- (00)frame-relay           Frame Relay Protocol
- (01)hdlc                 HDLC Protocol
- (02)ppp                 PPP Protocol
- (03)sdlc                 SDLC Protocol
- (04)x25                 X.25 Protocol

Please Input the code of command to be excute(0-4):

Then choose the protocol you want to encapsulate.

◆ **Configure Low-speed Serial Interface**

This section describes how to configure low-speed serial interface. Please see the “[Example of low-speed interface](#)“ for example of configuration.

Usually, the low-speed serial interface supports both synchronous mode and asynchronous mode. While in the status of interface configuring, use following command to assign the low-speed interface in the mode of synchronous or asynchronous:

Command	Function
<b>Physical-layer mode {sync  async}</b>	Assign the low-speed interface in the mode of synchronous or asynchronous

Choose the item 25 of prompt, it will display:

- (00)flow-control           Flow control
- (01)mode                 Configure sync or async physical layer on serial interface
- (02)sampling             set clock sampling mode
- (03)speed                 port speed

Please Input the code of command to be excute(0-3): **1**

Input 1,choose the item “ mode ” , it will prompt :

- (00)async                 asynchronous mode
- (01)sync                 synchronous mode

Please Input the code of command to be excute(0-1):

Input 0, choose the item “ async ” to set the interface as asynchronous type.

Input 1, choose the item “ sync ” to set the interface as synchronous type.

While in the mode of asynchronous, the low-speed serial interface supports all the commands of standard asynchronous interface. The default mode is synchronous. While in the status of interface configuring, use following command to return the mode of low-speed serial interface form asynchronous to synchronous:

Command	Function
<b>Physical-layer (default) mode</b>	Return to default mode----synchronous mode

Choose the item 25 of prompt, it will display:

U(undo) D(default) Q(quit)

- (00)flow-control           Flow control
- (01)mode                 Configure sync or async physical layer on serial interface

(02)sampling set clock sampling mode  
 (03)speed port speed

Please Input the code of command to be excute(0-3): **d**

Input D or d, it will prompt:

(00)flow-control Flow control  
 (01)mode Configure sync or async physical layer on serial interface  
 (02)sampling set clock sampling mode  
 (03)speed port speed

Please Input the code of command to be excute(0-3): **1**

Input 1,choose the item " mode ", it will prompt:

(00)async asynchronous mode  
 (01)<cr>

Please Input the code of command to be excute(0-1): **1**

Input 1,set it back to default mode.

While in the status of interface configuring, please use following command to configure the rate of synchronous mode and asynchronous mode:

Command	Function
<b>Physical-layer speed</b> <i>speed</i>	Assign the rate of interface

Choose the item 25 of prompt, it will display:

(00)flow-control Flow control  
 (01)mode Configure sync or async physical layer on serial interface  
 (02)sampling set clock sampling mode  
 (03)speed port speed

Please Input the code of command to be excute(0-3): **3**

Input 3, choose the item " speed ", then it will prompt various speed value, select the one you want.

The value of rate that supported by synchronous interface and asynchronous interface shown as following:

Synchronous interface	Asynchronous interface
1200,2400,4800,9600,14400,19200,38400,57600,64000,115200,128000,256000,512000,1024000,2048000	1200,2400,4800,9600,14400,19200,38400,57600,115200

### 3.8 Configuring E1 interface

#### ◆ Introduction of E1 interface

There are two types of configuration of E1 interface:

- To be treat as channelized E1 interface. The interface separates into 31 time-slots in physical and all the time-slots divide into several groups arbitrarily. Each group of time-slot is bind as one interface with the same logical characteristic of synchronous serial interface. Protocols of link layer are supported, which include PPP, frame relay, LAPB and X.25.
- To be treat as unchannelized E1 interface. As a G.703 synchronous serial interface with the rate of 2M in physical, The interface supports the protocols of link layer that include PPP, frame relay, LAPB and X.25.

#### ◆ Configuring E1 interface

To configure E1 interface, command **config-controller E1** must be inputed firstly in the status of global configuring.

Command	Function
---------	----------

<b>controller E1 &lt;slot&gt;/&lt;config-group&gt;</b>	Configure E1 interface slot is number of slot that controller located in, config-group is link number of E1 controller
--	--

Input the command “controller” , it will prompt:

```
(00)E1
Please Input the code of command to be excute(0-0): 0
Input 0, choose the item “ E1” , it will prompt:
(00)<2-2>
(01)<cr>
```

Please Input the code of command to be excute(0-1):  
Choose the corresponding item and input the slot number and group.

Example:

```
Router_config#config-controller E1 2/0
Router_config_controller_E1_2/0#
```

Configuring tasks of E1 interface include:

- Configure physical parameters of E1 interface that include frame check mode, line code/decode format and line clock, loop-back transmission mode, etc. Default parameter is required.
- Channelized E1 interface requires the configuring of parameter about set-channel-group and confirm the binding mode of time-slot.
- Unchannelized E1 interface has no need of configure the parameter of set-channel-group.
- Configure the parameter of interface.

◆ **Configuring Operation Mode of E1 Interface**

The default mode of E1 interface is channelized mode. It is able to set as unchannelized mode by the command of unframed.

Command	Function
<b>unframed</b>	Configure as unchannelized mode
<b>Unframed (undo)</b>	Configure as channelized mode

Choose item 30 of the prompt of interface parameters, then the interface will be configured as unchannelized mode.

If you input U or u before you do the action above, it will be configured as channelized mode.

Example:

```
Router_config#config-controller E1 2/0
Router_config_controller_E1_2/0# unframed
Router_config_controller_E1_2/0# no unframed
```

◆ **Configuring Frame Check Mode of E1 Interface**

E1 interface support CRC32 check for physical frame, default setting is unchecking.

Command	Function
<b>framing crc4</b>	Configure the frame checking of E1 interface as 4bytes CRC check.
<b>framing(undo) or framing no-crc4</b>	Configure the frame checking of E1 interface as unchecking.

Take the first command as an example:

Choose the item 13 of interface-parameter prompt, it will display:

```
(00)crc4
(01)no-crc4
```

Please Input the code of command to be excute(0-1): 0

Input 0 , choose the item "crc4".

#### ◆ Configuring Line Code/Decode Format of E1 Interface

There are two formats of line code/decode supported by E1 interface: AMI and HDB3

Default setting is HDB3.

Command	Function
<b>line code ami</b>	Configure line code/decode format of E1 interface as AMI
<b>line code (undo) or line code hdb3</b>	Configure line code/decode format of E1 interface as HDB3

Choose item 19 of interface-parameter prompt, it will prompt:

(0)ami use ami mode

(01)hdb3 use hdb3 mode

Please Input the code of command to be excute(0-1):

Choose 0 , it will be set as ami format ;

Choose 1 , it will be set as hdb3 format.

#### ◆ Configuring Line Clock of E1 Interface

If E1 interface is operated as synchronous interface, two operation modes available for E1 that is of DTE and DCE. It is need to choose line clock. While two Routers straight connected with E1 interfaces, the two ports must be operated with DTE and DCE separately. While Router connects with Exchange through E1 interface, DCE for Exchange and DTE for E1 interface of Router.

Default operation mode of E1 interface is DTE.

Command	Function
<b>clock internal</b>	Configure operation mode of E1 interface as DCE that use internal synchronous signal of chip.
<b>clock external</b>	Configure operation mode of E1 interface as DTE that use synchronous signal of line.

Choose item 5 of interface-parameter prompt, it will display:

(0)external external clock

(01)internal internal clock

Please Input the code of command to be excute(0-1):

Choose 0, use internal synchronous signal of chip;

Choose 1 , use synchronous signal of line.

#### ◆ Configuring Loopback Transmission Mode of E1 Interface

While in the mode of remot loop-back transmission, the message that received through the port will be return by E1 through the sending channel.

Command	Function
<b>loopback local</b>	Configure the operation mode of E1 as remote loop-back
<b>Loop(undo)</b>	Cancel the setting of remote loop-back

Take the first command as an example:

Choose the item 20 of interface-parameter prompt, it will display:

(00)local set local loopback

(01)remote set local remoteback

Please Input the code of command to be excute(0-1): **0**

Input 0, choose the item “local” .

◆ **Configuring Transmitting Impulse Mode of E1**

Choose transmitting impulse mode. To execute **Cable 120** for cable type is 1200 twisted-pair. The 750 coaxial cable for default setting and obey ITU-T G.703 standard. The transmitting impulses of two types of cable are different.

Command	Function
<b>Cable 120</b>	Configure the cable of E1 interface as 1200 twisted-pair
<b>No cable</b>	Default setting is 750 coaxial cable

Choose item 1 of interface-parameter prompt, it will display:

(00)120 set 120ohm cable

Please Input the code of command to be excute(0-1): **0**

Choose 0.

◆ **Forbid the link of E1 interface**

Use for forbidding a E1 interface and the line status for all interfaces of port switch to *down*.

Command	Function
<b>Shutdown</b>	Forbid the link of E1 interface
<b>Shutdown(undo)</b>	Restore the link of E1 interface

Choose item 28 of interface-parameter prompt, then the link will be forbidden. If you input the “U” or “u” before choose the item 28, the link will be resumed.

Example:

Router\_config#config-controller E1 2/0

Router\_config\_controller\_E1\_2/0#shutdown

Router\_config\_controller\_E1\_2/0# shutdown(undo)

◆ **Configuring set-channel-group Parameter of E1 Interface**

set-channel-group is channel number of E1 with the range of 0-30. the timeslot is time-slot number of E1 with the ranger of 1-31. The channel is able to occupy any non-assigned time-slot and combines time-slot arbitrarily. The configuration of E1 channel will generate new interface.

The binding time-slot of channel-group will be cleared by no channel-group. The corresponding interface will be cleared too.

Command	Function
<b>Channel</b> <i>channel-group</i> <b>timeslots</b> { <i>number</i>   <i>number1-number2</i> } [ <i>number</i>   <i>number1-number2</i> ... ]	Bind the time-slot of E1 interface to set-channel-group
<b>Channel(undo)</b> <i>channel-group</i>	Cancel the time-slot binding of channel-group

Choose the item 2 of interface-parameter prompt, it will display:

(00)<0-30> Channel number

Please Input the code of command to be excute(0-1): **0**

Choose 0 and input the channel number, it will prompt :

(00)timeslots

Please Input the code of command to be excute(0-1): **0**

Input 0 , choose the item “timeslots” , it will prompt :

(00)<1-31> List of timeslots which comprise the channel

Please Input the code of command to be excute(0-1): **0**

Choose 0, the configuration is correct.

Example:

```
Router_config#config-controller E1 2/0
Router_config_controller_E1_2/0#channel 5 timeslots 18,11-13,20,22,30-28,24-25
Router_config_controller_E1_2/0#config-interface s2/0:5
Router_config_interface_s2/0:5#
```

#### ◆ Configuring Interface Parameter of E1 Interface

- While the E1 interface in the Channelized mode, system will generate new interface after configure the channel-group parameter with the same logical characteristic of synchronous serial interface. The name is serial<slot>/<group>:<channel-group>. The <slot> and <group> is the same as controller E1 <slot>/<group>.
- While the E1 interface in the Unchannelized mode, system will generate new interface with the name is serial<slot>/<group>:0. it is able to encapsulate the data-link-layer protocol to the interface, which include PPP, frame relay, HDLC and X.25, etc.

Example:

In Channelized mode:

```
Router_config#config-controller E1 2/0
Router_config_controller_E1_2/0#channel 1 timeslots 1-31
Router_config_controller_E1_2/0#int s2/0:1
Router_config_controller_s2/0:1#enca fr
Router_config_controller_s2/0:1#ip add 130.130.0.1 255.255.255.0
```

In Unchannelized mode:

```
Router_config# controller E1 2/0
Router_config_controller_E1_2/0#unframed
Router_config_controller_E1_2/0#int s2/0:0
Router_config_controller_s2/0:0#enca fr
Router_config_controller_s2/0:0#ip add 130.130.0.1 255.255.255.0
```

#### ◆ Configuring the PRI interface

Introduction of PRI interface

PRI interface is a kind of ISDN interface which consists of 30 B channels plus a singled channels.. The number of the B channel of our PRI interface is not fixed as 30 but can be set by user to meet their requirement. You can generate and delete the PRI interface through the E1 interface, it's dynamic. You can set the detailed timeslot as a B channel of a general serial port or a PRI interface through the command line. When one or more timeslot has been configured as the PRI B channel of an E1 interface, the fifteenth timeslot will always be utilized by the PRI interface as the D channel of signal alternation.

To configure the PRI interface, you must input the command “ **controller E1** ” in the global configurative mode firstly.

Command	function
<pre>controller E1 &lt;slot&gt;/&lt;group&gt;</pre>	Configure E1 interface <b>Slot</b> is the slot number of E1 controller <b>Group</b> is the link number of E1 controller
<pre>Pri-group timeslot num</pre>	num: you can assign many timeslot to one B channel. If those timeslots are continuous, use the “ - ” to connect them. Else , use “ , ” .

Command 1 :

Input the command “ **controller** ” , it will prompt:

```
(00)E1
```

```
Please Input the code of command to be excute(0-0): 0
```

Input 0, choose the item “ E1” , it will prompt:

(00)<2-2>

(01)<cr>

Please Input the code of command to be excute(0-1):

Choose the corresponding item and input the slot number and group.

Command 2 :

Choose the item 22 of parameter prompt, it will display:

(00)timeslots

Please Input the code of command to be excute(0-0): **0**

Input 0 , choose the item “timeslot” , it will prompt:

(00)<1-31> List of timeslots which comprise the channel

Please Input the code of command to be excute(0-0): **0**

Choose the item 0, then input “num”.

This command is used to set up a main workgroup and assign timeslots for the main workgroup. All the timeslots can be assigned to B channel except 0 and 16. Each timeslot is a correspondence of a B channel while each B channel is also a correspondence of a virtual 64K connection according to the protocol encapsulated by D channel. You can ' t configure the D channel until you have set up a main workgroup and assigned timeslots for B channels.

The configurative method of entering the D channel is : int serial slot/port:15。 After you enter the D channel, you can encapsulate protocol, set dial-up group and set the dial-up mapping of peer.

### 3.9 Configure the BRI interface

#### ◆ introduction of BRI interface

BRI is a kind of ISDN interface which consists of a single D channel plus 2 B channels. The D channel is used to set up B channels and signal alternation channel of the interface. B channels are used to transfer data.

#### Configuration of BRI interface

To configure the BRI interface ,you must under the ISDN BRI configurative mode firstly.

command	function
interface bri <slot>/<group>	Enter the ISDN BRI interface Slot is the slot number of BRI controller Group is the link number BRI controller

Input the command “**interface**”, it will prompt:

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)BRI ISDN Basic Rate Interface

.....

Please Input the code of command to be excute(0-11): **2**

Input 2, choose the item “ BRI”, it will prompt:

Please input a interface name:

Input the interface type, slot number and group.

### 3.10 Configure DTU interface

This section describes how to configure the DTU interface. 1750,2620 and 2630 series router support DTU interface. Detailed configurative steps are given below:

#### Designating DTU interface

You can input the following command in global configurative mode to enter the DTU interface configurative mode.

command	function
interface bm <slot>/<port>	Configure the DTU interface

For example :

Input the command “ interface” , it will prompt:

(00)FastEthernet      FastEthernet interface

(01)Ethernet          Ethernet interface

(02)Serial            Serial interface

(03)Async            Asynchronous interface

(04)BM                BM interface

.....

Please Input the code of command to be excute(0-10): **4**

Input 4, choose the item “ BM” , it will prompt:

Please input a interface name: **bm2/0**

Input “bm2/0” .

#### ◆ Configuring DTU interface ' s linemode

command	Function
<b>linemode nt</b>	Set the DTU interface working in NT mode
<b>linemode lt</b>	Set the DTU interface working in LT mode

The DTU is in NT mode in default.

For example : configure the DTU interface working in LT mode.

Choose the item 21 of the interface-parameter prompt, it will display:

(00)nt                nt mode

(01)lt                lt mode

Please Input the code of command to be excute(0-1): **0**

Input 1, choose the item “ lt” .

#### ◆ Configuring speed of the DTU interface

command	function
<b>physical-layer speed</b> speed	Designate the interface speed

Choose the item 26 of the interface-paramter prompt, it will display:

(00)flow-control    Flow control

(01)mode            Configure sync or async physical layer on serial interface

(02)sampling        set clock sampling mode

(03)speed           port speed

Please Input the code of command to be excute(0-3): **3**

Input 3, choose the item and input the speed.

The supported speed are listed below:

speed	specification
64000 , 128000	64000 (default)

For example :

Configure the speed of DTU interface as 128K.

**router\_config bm2/0#physical-layer speed 128000**

### 3.11 configuring the MODEM interface

This section describes how to configure the MODEM interface. It includes:

#### Designating MODEM interface

You can input the following command in the global configurative mode to enter the MODEM interface configurative mode.

command	function
<code>interface async &lt;slot&gt;/&lt;port&gt;</code>	Configuring the MODEM interface

For example :

Input the command “interface”, it will prompt:

- (00)FastEthernet      FastEthernet interface
- (01)Ethernet          Ethernet interface
- (02)Serial             Serial interface
- (03)Async              Asynchronous interface

.....

Please Input the code of command to be excute(0-10): **3**

Input 3, choose the item “Async”, it will prompt:

Please input a interface name: **async2/0**

Input “async2/0”.

MODEM interface is conceived as a general asynchronous interface which connect with a external MODEM in the system. Refer to the configuring asynchronous interface and dial-up interface for more detail.

### How to connect with V.92 MODEM or those that doesn ' t support V.42bis

Since the chip of our MODEM card can not support the protocol beyond V90, if you want to connect with some V.92 MODEM of other company, the connection with the V.92 MODEM may be failed. (however, you can still dial from the V.92 MODEM to the router.). User can write an initializing script, add “AT&H4 OK” into it. Then, the network mode of MODEM will be adjusted to V.32bis multimode and the connection with V.92 MODEM can be set up successfully. You can also use this method when you can not create connection with other older MODEM. What’s more, if the MODEM of peer does not support V.42bis encapsulation protocol, you can close the encapsulation function by adding “AT%C0 OK” into the initializing script. The network mode and command type are listed below:

command	Network mode
AT&H0	V.92 multimode
AT&H1	V.90/V.34
AT&H2	V.34 multimode
AT&H3	V.34 only
AT&H4	V.32bis multimode
AT&H5	V.32bis only
AT&H6	V.22bis
AT&H7	V.22
AT&H8	Bell 212
AT&H9	Bell 103
AT&H10	V.21
AT&H12	V.23

#### ◆ Configuring Logical Interface

In this section we will introduce how to configure the logical interface that include following content:

#### ◆ Configuring a Null Interface

The D-Link router supports a "null" interface. This pseudo-interface functions similarly to the null devices available on most operating systems. This interface is always up and can never forward or receive traffic. The only interface configuration command that you can specify for the null interface is **no ip unreachable**. The null interface provides an alternative method of filtering traffic. You can avoid the overhead involved with using access lists by directing undesired

network traffic to the null interface.

To specify the null interface, use the following command in global configuration mode:

Command	Function
<b>interface null</b>	Enter the status of null interface configuring

Input the command “ interface ” , it will prompt:

```
(00)FastEthernet    FastEthernet interface
(01)Ethernet        Ethernet interface
(02)Serial          Serial interface
(03)Async           Asynchronous interface
(04)Null            Null interface
```

.....

Please Input the code of command to be excute(0-10): **4**

Input 4, choose the item “Null”, it will prompt:

Please input a interface name: **null0**

Input “null0”.

The null interface can be used in any command that has an interface type as an argument. The following example configures a null interface for IP route 192.168.20.0.

```
ip route 192.168.20.0 255.255.255.0 null 0
```

#### ◆ Configure a Loopback Interface

A loopback interface is a logical interface that is always up and allows BGP sessions to stay up even if the outbound interface is down. You can use the loopback interface as the termination address for BGP sessions. In applications where other routers or access servers attempt to reach this loopback interface, you should configure a routing protocol to distribute the subnet assigned to the loopback address. Packets routed to the loopback interface are rerouted back to the router and processed locally. IP packets routed out the loopback interface but not destined to the loopback interface are dropped. This means that the loopback interface serves as the Null interface also.

To specify a loopback interface and enter interface configuration mode, use one of the following commands in global configuration mode:

Command	Function
<b>interface loopback <i>number</i></b>	Enter the status of loop-back interface configuring

Input the command “ interface ” , it will prompt:

```
(00)FastEthernet    FastEthernet interface
.....
(05)Loopback        Loopback interface
```

.....

Please Input the code of command to be excute(0-10): **5**

Input 5 , choose the item “Loopback”, it will prompt:

Please input a interface name:

Input the “loopback interface”.

#### ◆ Configure Dialup Interface

The dialup interface is a kind of logical interface, which configure the dialup setting of multiple physical interfaces in one virtual interface. Thereby, the dialup interface will builds the communication of physical interface and dialup interface to manage multiple interfaces in the same time.

Use following command to configure dialup interface:

Command	Function
<b>interface dialer</b> <i>number</i>	Enter the status of dialup interface configuring
<b>dialer rotary-group</b> <i>number</i>	Set the communication of dialup interface and physical interface

**Command 1:**

Input the command “interface” in global configurative mode, it will prompt:

(00)FastEthernet           FastEthernet interface

.....

(07)Dialer                   Dialer interface

.....

Please Input the code of command to be excute(0-10): **7**

Input 7, choose the item “ Dialer” , it will prompt:

Please input a interface name:

Input the dialer number.

**Command 2 :**

Set the interface to dial-up, choose the item “ Dialer” of prompt, it will display:

(00)called                   Dialer called string

.....

(09)rotary-group           Add this interface to a dialer rotary group

.....

Please Input the code of command to be excute(0-28): **9**

Input 9 , choose the item “ rotary-group” , it will prompt:

(00)Dialer                   Dialer interface

Please Input the code of command to be excute(0-0): **0**

Input 0 , choose the item “ Dialer” , it will prompt:

Please input a interface name:

Input string.

◆ **Configuring Virtual template and Virtual access interface**

Virtual template and virtual access interface

Virtual template and virtual access interface are two partnership interfaces. The Virtual access interface is created for protocol requirement, its configurative information originate from the configuration of virtual template interface. Virtual template and virtual access interface are generally used in some special case such as protocol conversion(for example, PPP over X.25) and Multilink PPP and so on.

You can use the following command to define the virtual template interface:

command	function
<b>Interface virtual-template</b> <i>number</i>	Configure the virtual template interface

Input the command “interface”, it will prompt:

(00)FastEthernet           FastEthernet interface

.....

(09)Virtual-template           Virtual template interface

.....

Please Input the code of command to be excute(0-10): **9**

Input 9, choose the item “ Virtual-template”, it will prompt :

Please input a interface name: **Virtual-template**

Input Virtual-template , it will prompt :

Please Input the code of command to be excute(0-0): **0**

Input 0, it will prompt:  
Please input a interface name:1  
Input number.

#### ◆ Configure the Multilink interface

Multilink interface

Multilink interface is defined in allusion to Multilink PPP. This interface is usually used for the Multilink PPP of a serial interface.

User the following command to define the multilink interface:

Command	Function
Interface multilink <i>number</i>	Configure the multilink interface

Input the command “interface”, it will prompt:

```
(00)FastEthernet      FastEthernet interface
.....
(08)Multilink         Multilink-group interface
.....
```

Please Input the code of command to be excute(0-10): **8**

Input 8, choose the item “multilink”, it will prompt:

Please input a interface name: **Multilink**

Input “Multilink” , it will prompt :

```
(00)<0-32767>  Multilink interface number
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , it will prompt :

Please input a interface number:

Input “number”

#### ◆ Configure the Tunnel interface

Tunnel interface

Tunnel interface is defined for some encapsulated protocol. The current version supports the encapsulation protocol of GRE/Ip type.

To designate a Tunnel interface and enter the interface configurative mode, use the following command in the global configurative mode:

command	Function
Interface Tunnel <i>number</i>	Configure the Tunnel interface

Input the command “interface”, it will prompt:

```
(00)FastEthernet      FastEthernet interface
.....
(06)Tunnel           Tunnel interface
.....
```

Please Input the code of command to be excute(0-10): **6**

Input 6 , choose the item “Tunnel” , it will prompt:

Please input a interface name: **Tunnel**



### Configuration of ROUTER B

```
int f0/0.1
  encapsulation dot1q 2
  ip address 192.168.20.22 255.255.255.0
```

### Configuration of ROUTER C

```
int f0/0.1
  encapsulation dot1q 1
  ip address 192.168.20.33 255.255.255.0
```

### Configuration of ROUTER D

```
int f0/0.1
  encapsulation dot1q 2
  ip address 192.168.20.44 255.255.255.0
```

With this configuration, A is only to PING with C each other and B is only to PING with D each other.

### Example of PRI interface configuring

```
router _config# control e1 3/2 (enter the E1 configurative mode)
router _config _controller# pri-group timeslot 1-5,9,10
router _config _controller#int s3/2:15 (enter the D channel configurative mode).
```

### Example of BRI interface configuring

```
router _config# interface b3/2 (enter the isdn bri interface configurative mode)
router _config _b3/2#dialer string 222
```

## 3.12 Configuring SNMP List

- ◆ SNMP system consist of 3 parts as below:
  - SNMP Network Management System (NMS)
  - SNMP agent
  - Management Information Base (MIB)
- ◆ SNMP is link layer protocol. It provides the message format that use for communication of SNMP management port and SNMP agent.
- ◆ SNMP management port can be considered as a part of Network Management System (NMS, such as D-LinkWorks). The agent and MIB reside in Router. It is need to define the relation of management port and agent before configure SNMP of Router.
- ◆ SNMP agent contains MIB variable and the agent is able to query and change these variable values. The management port acquires variable value from agent or stores variable value to agent. The agent collects data from MIB. MIB is the information base of equipment parameter and network data. MIB can also responses the requirement of data reading or data setting from management port. SNMP agent send trap to management port actively. The trap is alert message about some situation of network that sends to SNMP management port that is of some situation of network. The trap is used to point out incorrect user authentication, restart, status of link (startup or closed), closedown of TCP link, lose the link of adjacent Router and/or other important matters.

### SNMP Notification

- ◆ To send inform to SNMP management port while special occurrence. For example, the agent Router sends a message to management port if the agent encounters an error condition.
- ◆ SNMP notification can be sent as trap or inform request. Because receiving port did not send any response when the trap was received, thereby, the sending port could not confirm whether the trap was received or not.

Thus, the trap is unreliable. Oppositely, the management port of inform request receiving will adopt SNMP responded PDU as responson of this message. If the management port di not receive a inform request, then the responson will not to be sent. If the sending port did not receive the responson, the inform request will be resent. Thus, the notification has more possibility that to be sent to planned destination

- ◆ The inform request occupied more resource of Router and network because it is more reliable. The trap will be discarded as soon as it is sent. Another side, inform request must be saved in memory until the system received responson or request overtime. In addition, the trap can only be sent once but inform request can be sent many times. The retransmission increased the communication traffic of network and generated more burthen. Therefore, the trap and inform request balance the reliableility and resource. The inform request can be chose if SNMP management port extremely need to receive each notification. If communication traffic of network or memory of Router is more important and need not to care each notification, trap is the better choice.
- ◆ D-Link Router presently supports trap but also provides the extension of inform request.

**Version of SNMP**

D-Link Router presently supports following SNMP versions:

SNMPv1---Simple Network Management Protocol. A full standard of internet defined in RFC1157.

SNMPv2C--- Community based management frame of SNMPv2. Test protocol of internet that defined in RFC1901.

D-Link Router support following SNMP versions:

SNMPv3 .

SNMPv1 utilizes community based security mode to access management port that the agent of MIB. The community is definted by IP address Access Control List and password. The agent of SNMP must be configured as the version that supported by management workstation. The agent is able to communicate with various management ports.

**Supported MIB**

D-Link SNMP supports the entire MIB II variable (described at RFC 1213) and SNMP trap (described at RFC 1215).

D-Link provides private MIB extension for each system.

**Creat or modify the access control for SNMP community**

- ◆ The relation of SNMP management port and agent is definted by SNMP community character string. The community character string similar as the password that allows accessing the agent of Router. The optional item is to assign one or several features concern with community character string as below:
- ◆ Community character string is allowed to acquire the IP address access list of SNMP management port with authority of agent access.
- ◆ To define the MIB view for the entire MIB object subset with accessing authority of assigned community.
- ◆ Assign the read/write authority of community that has the authority to access MIB object.
- ◆ Configure community character string in the mode of global configuration:

Command	Function
<code>snmp-server community string [view view-name] [ro   rw] [word]</code>	Define the community accessing character string

Input the command “ **snmp-server** ” , it will prompt:

U(undo) D(default) Q(quit)

- (00)community            Enable SNMP; set community string and access privs
- (01)contact             Text for mib object sysContact
- (02)host                 Specify hosts to receive SNMP TRAPs

.....

Please Input the code of command to be excute(0-8): **0**

Input “ 0 ” , choose the item “ community ” , it will prompt:

(00)WORD                 SNMP community string

Please Input the code of command to be excute(0-0): **0**

Input 0 , choose the item “ WORD ” , it will prompt:

Please input a string:

Input the string , then it will prompt :

- (00)WORD               Std IP accesslist allowing access with this community string
- (01)ro                 Read-only access with this community string
- (02)rw                 Read-write access with this community string
- (03)view               Restrict this community to a named MIB view
- (04)<cr>

Please Input the code of command to be excute(0-4):

Choose the parameter you want to configure.

One or more community can be configured. Use the command **no snmp-server community** to erase the given community character string.

Please see the section "[SNMP command](#)" to get more examples about configuration of community character string.

#### ◆ Set the contact information of the route's administrator and location of Router

sysContact and sysLocation are all management variable of system group in MIB and respectively define the operator ID and actual location of managed node (Router). The user can access the information through the configuring file. One or several commands below will be used in the mode of global configuration:

Command	Function
<b>snmp-server contact</b> <i>text</i>	Set the character string of node operator
<b>snmp-server location</b> <i>text</i>	Set the character string of node location

Input the command " SNMP server " , it will prompt:

- (00)community        Enable SNMP; set community string and access privs
- (01)contact         Text for mib object sysContact
- (02)host             Specify hosts to receive SNMP TRAPs
- (03)location         Text for mib object sysLocation

.....

Please Input the code of command to be excute(0-8): **1**

Input " 1 " , choose the item " contact " , it will prompt:

- (00)LINE             identification of the contact person for this managed node

Please Input the code of command to be excute(0-0): **0**

Input 0, choose the item " LINE " , it will prompt:    Please input a string:

Input the contact string.

Input the command snmp-server, it will prompt:

- (00)community        Enable SNMP; set community string and access privs
- (01)contact         Text for mib object sysContact
- (02)host             Specify hosts to receive SNMP TRAPs
- (03)location         Text for mib object sysLocation

.....

Please Input the code of command to be excute(0-8): **3**

Input 3 , choose the item " contact " , it will prompt:

- (00)LINE             identification of the contact person for this managed node

Please Input the code of command to be excute(0-0): **0**

Input 0 , choose the item " LINE " , it will prompt:

Please input a string:

Input the location string.

#### ◆ Define the maxium length of SNMP agent data packet

The permitted maxium length of data packet can be set while SNMP agent receiving request or sending responson. Use

following command in the mode of global configuration:

Command	Function
<b>snmp-server packetsize</b> <i>byte-count</i>	Set the permitted maximum length of data packet.

Input the command " snmp-server ", it will prompt:

```
(00)community      Enable SNMP; set community string and access privs
.....
(04)packetsize     Largest SNMP packet size
.....
```

Please Input the code of command to be execute(0-8): **4**

Input 4, choose the item " packetsize ", it will prompt:

```
(00)<484-17940>    Packet size
```

Please Input the code of command to be execute(0-0): **0**

Input 0, it will prompt:

Please input a digital number:Please input a string:

Input the maximum length of a data packet.

#### ◆ Supervise the status of SNMP

Use following command in the mode of global configuration to supervise the statistics about input and output of SNMP, which is include the list of illegal community character string, amount of error and request variable.

Command	Function
<b>show snmp</b>	Supervise the status of SNMP

Input the command " show ", all the parameters will be listed:

```
(00)alias          alias for command
.....
(33)snmp          SNMP statistics
.....
```

Please Input the code of command to be execute(0-45): **33**

Input 33, choose the item " snmp ", it will prompt:

```
(00)host          show SNMP trap hosts
(01)view          show SNMP views
(02)<cr>
```

Please Input the code of command to be execute(0-2):

Choose the content you want to show.

#### ◆ Configure SNMP trap

To use following command to configure the SNMP trap that sent by Router, (the second task is optional):

Configure the Router-send trap

Change the parameter of trap running

#### ◆ Configure the Router-send trap

Use following command in the mode of global configuration, which is configures the Router to send a trap to a host.

Command	Function
<b>snmp-server host</b> <i>host community-string [udp-port port]</i> <i>[trap-type]</i>	Assign the receiver of trap message.

Input the command " snmp-server ", it will prompt:

```
(00)community      Enable SNMP; set community string and access privs
(01)contact        Text for mib object sysContact
(02)host           Specify hosts to receive SNMP TRAPs
```

.....

Please Input the code of command to be excute(0-8): **2**

Input 2, choose the item "host", it will prompt:

(00)Hostname or A.B.C.D                      IP address of SNMP TRAP host

Please Input the code of command to be excute(0-0): **0**

Input 0 , it will prompt:

Please input a string:

Input the Hostname or IP address , it will prompt:

(00)WORD                      SNMP community string

Please Input the code of command to be excute(0-0): **0**

Input 0, choose the item " word ", it will prompt:

Please input a string:

Input string, it will prompt:

- (00)authentication              Allow authentication failure traps
- (01)configure                      Allow SNMP-configure traps
- (02)snmp                              Allow SNMP-type traps
- (03)<cr>

Please Input the code of command to be excute(0-3):

Choose the aimed trap-type.

- ◆ The SNMP agent will automatic boot after switch on D-Link Router and then activate all types of trap. Use the command **snmp-server host** to assign the type of traps and the receiving host.
- ◆ Some traps must be control by other commands. For example, if the SNMP link trap needs to be sent while open or close the interface, so that the command **snmp trap link-status** is used for activate link trap in the mode of interface configuring. The interface configuring command **no snmp trap link-stat** is used for close these traps.
- ◆ The host must be configured with the command **snmp-server host** for receiving traps.

### Change the running parameter of trap

As option, the command is use for assign the source interface to generate traps, and then assign each host with the queue length of message (data packet) or value of retransmission interval. Use following optional command in the mode of global configuration to change the running parameter of trap:

Command	Function
<b>snmp-server trap-source</b> <i>interface</i>	Assign the source interface (include IP address) for generating of trap message. This command is also sets resource IP address for message.
<b>snmp-server queue-length</b> <i>length</i>	Create message queue length for each trap host.
<b>snmp-server trap-timeout</b> <i>seconds</i>	Define the frequency of the retransmitting trap message that in the retransmitting queue.

Take the first command for example, input the command " snmp-server " , it will prompt:

- (00)community                      Enable SNMP; set community string and access privs
- .....
- (06)trap-source                      Assign an interface for the source address of all traps
- .....

Please Input the code of command to be excute(0-8): **6**

Input 6, choose the item " trap-source " , it will prompt:

- (00)FastEthernet                      FastEthernet interface
- (01)Ethernet                              Ethernet interface
- (02)Serial                                  Serial interface

(03)Async                      Asynchronous interface  
 (04)Null                        Null interface

Please Input the code of command to be excute(0-4):

Choose and input the type, slot and port number of the interface.

### Example of configuration

#### ◆ Example 1:

```
snmp-server community public RO
snmp-server community private RW
snmp-server host 192.168.10.2 public
```

There are two community character strings that to be configured in this example. One is “public” that has the authority to read all of MIB variable; another is “private” that has the authority to read/write all of MIB variable. User is able to read the MIB variable in Router by “public”, and read the variable or write the writable variable in Router by “private”. While the Router is need to send trap message, it is also assign that use public send trap message to 192.168.20.2. For example, the Router will send trap message “linkdown” to 192.168.20.2 when a port of Router is down.

#### ◆ Example 2:

```
snmp-server community public view sysmib RO
snmp-server community private RW nativehost
snmp-server contact D-Link@D-Link.com.cn
snmp-server host 192.168.10.2 public snmp
snmp-server location 405-D-Link
snmp-server view sysmib system included
ip access-list standard nativehost
permit 192.168.10.2 255.255.255.255
```

In this example, the community character string “public” only has the authority to read the MIB variable of the Router’s system group. Only the host with IP address 192.168.10.2 is allowed to read/write the MIB variable of Router’s system group by the community character string “private”. Only the “snmp” trap message is sent to the host with IP address 192.168.10.2. The trap message “authentication” or “configure” will not to be sent to host. To set the contact information asD-Link@D-Link.com.cn with location of 405-D-Link, that is, D-Link@D-Link.com.cn is the value of MIB variable “sysContact” in system group, and the value of sysLocation is 405-D-Link.

## 3.13 configuring the CDP

This chapter describes how to configure the CDP function of D-link router.

CDP is a media and protocol-independent protocol that can be used to detect all the devices directly attached to the router. Network management applications can retrieve the device type and SNMP-agent address of neighboring device using CDP.

The CDP function of D-link router can implement the detection of neighboring devices. However, it can not query neighboring devices by SNMP. Hence, the D-link router can only be put on the network end, otherwise, it wouldn’t get the whole network topology structure.

The CDP can configured on all the SANP (such as Ethernet, HDLC, Frame Relay, PPP and so on).

### CDP default configuration

function	Default configuration
CDP global configurative mode	Disable
CDP interface configurative mode	Disable
CDP clock ( message interval )	60 seconds
CDP holdtime	180 seconds

## Set the CDP message interval and holdtime

You can use the following commands in global configurative mode to set CDP message interval and holdtime:

step	command	function
1	<code>pdp timer seconds</code>	Configuring the message interval of CDP
2	<code>pdp holdtime seconds</code>	Configuring the CDP message holdtime

Here is an example :

```
[DEFAULT@Router /config/]#pdp
```

```
(00)holdtime          specify the hold time to be sent in packets
(01)run               enable PTOPO discovery protocol to run
(02)timer             specify the interval at which packets are sent
```

Please Input the code of command to be excute(0-2): **2**

```
(00)<5-254>          time interval(in seconds)
```

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:Please input a string:**100** (input the “time interval” you want ,here is only an example)

Will you excute it? (Y/N):**y**

```
[DEFAULT@Router /config/]#pdp
```

```
(00)holdtime          specify the hold time to be sent in packets
(01)run               enable PTOPO discovery protocol to run
(02)timer             specify the interval at which packets are sent
```

Please Input the code of command to be excute(0-2): **0**

```
(00)<10-255>         length of time(in seconds)
```

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:Please input a string:**30** ( input a holdtime you want, here is an example ) .

Will you excute it? (Y/N):**y**

Enable CDP

Cdp is disable in default configuration. If you want to use CDP function, implement the following command in global configurative mode:

Command	Purpose
<code>pdp run</code>	Enable CDP function of the router

Example :

```
[DEFAULT@Router /config/]#pdp
```

```
(00)holdtime          specify the hold time to be sent in packets
(01)run               enable PTOPO discovery protocol to run
(02)timer             specify the interval at which packets are sent
```

Please Input the code of command to be excute(0-2): **1**

Will you excute it? (Y/N):**y**

enable the CDP on a port

cdp is disable in default configuration. When the CDP function of the router is enabled, you can also enable the CDP on a port. Use the following command in interface configurative mode:

command	function
<code>pdp enable</code>	Enable the CDP function on a port

Key Word:

Q(quit)

```

.....
(23)pdp                                pdp configuration commands
(24)physical-layer                      Configure physical layer parameters
.....
Please Input the code of command to be excute(0-32): 23
Key Word:
U(undo)  D(default)                    Q(quit)
(00)enable                               Enable pdp on interface
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y

```

## monitoring and managing CDP

In order to monitoring CDP, you can use the following commands in management mode:

command	Function
show pdp traffic	Show the traffic of CDP packet transmitted or received by router
show pdp neighbor [detail]	Show all the neighbor detected by CDP

Example 1 :

```

[DEFAULT@Router /enable/]#show
Key Word:
U(undo)  D(default)                    Q(quit)
.....
(27)memory                               memory info
(28)pdp                                   pdp State information
.....
Please Input the code of command to be excute(0-49): 28
Key Word:
Q(quit)
(00)neighbor                             pdp neighbor information
(01)traffic                              pdp statistics
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y

```

Example 2 :

```

[DEFAULT@Router /enable/]#show
.....
(27)memory                               memory info
(28)pdp                                   pdp State information
.....
Please Input the code of command to be excute(0-45): 28
(00)neighbor                             pdp neighbor information
(01)traffic                              pdp statistics
Please Input the code of command to be excute(0-1): 0
(00)detail                               Show detailed information
(01)<cr>
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y

```

## Example of CDP configuration

### Enable CDP function

```
[DEFAULT@Router /config/]# pdp run
[DEFAULT@Router /config/]# int f0/0
[DEFAULT@Router /f0/0/]# pdp enable
configuring the CDP message interval and message holdtime
[DEFAULT@Router /config/]# pdp timer 30
[DEFAULT@Router /config/]# pdp holdtime 90
monitoring CDP message
[DEFAULT@Router /enable/]# show pdp neighbors
Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H -
Host, I - IGMP, r - Repeater
Device ID Local InfrfceHoldtmeCapabilityPlatform Port ID
joeEth 0 133 4500 Eth 0
samEth 0 152 R AS5200 Eth 0
```

### 3.14 Directory of VTY configuration

#### Introduction of VTY configuration

D-Link Router utilize command *line* to configure the terminal parameter in simple and agile. The process of configuration coincides with the habit of user. The setting of width and height can be displayed to terminal in command *line*.

#### Software configuration

In this section, we will introduce how to configure pseudo terminal. Please see the chapter “VTY command” to get more configuring commands of pseudo terminal.

#### Configuring task

D-Link Router has four types of circuit: console, auxiliary, asynchronization and virtual terminal circuit. The different Router has different amount of above-mentioned circuit. Following are references about correctly configure the software and hardware.

Type	Interface	Description	Rule of circuit numbering
CON(CTY)	Console	Use for login the Router and configuring.	Number 0
AUX	Assistant	RS-232 DTE port is use for backup asynchronous port (TTY) and cannot be use as the second console port.	Number: less than (or equal to) 4 slots is 65. Otherwise, it is accounted as the number slot multiplied by 16 and then adds one.
TTY	asynchronization	This is asynchronous interface. Usually use for dialup conversation with SLIP and PPP remote contact.	Start number is 1. The amount of number will change with variation of platform. The range of number is maxium asynchronous interfaces that Router supported. For example, No. 1 slot has 16 asynchronous modules, No. 2 slot is empty, and No. 3 has 8 synchronous modules. Thus, a1/0 correspond to line 1, a1/15 correspond to line 16,s3/0 correspond to line 17 and s3/7 correspond to line 24.
VTY	Virtual asynchronization	Use for connect to Telnet, X.25 PAD, HTTP and Rlogin of synchronous port of Router (such as Ethernet and serial interface).	The 64 numbers that form maxium number of TTY circuit and add one.

- ? Asynchronous interface and TTY circuit
- ? Synchronous interface and VTY circuit

- ◆ Asynchronous interface and TTY Asynchronous interface correspond to physical terminal circuit [TTY]. Asynchronous interface can be connecting with terminal while protocol is not encapsulated.
- ◆ Synchronous interface and VTY circuit: Virtual terminal circuit provides to access Router through the synchronous interface. Corresponding of VTY circuit to synchronous interface is different from TTY circuit to asynchronous interface. The reason is VTY circuit is dynamic created in Router but TTY circuit is static physical port. While a user connects to Router through VTY circuit, the user is connecting a virtual port of interface. Every asynchronous interface has multiple virtual ports if it is permitted.

For example, several Telnet connect to a interface [Ethernet or serial interface].

Following operations are needed for VTY configuration:

- ? enter the mode of line configuring
- ? configure terminal parameter

Please see the section of " [Example of VTY configuration](#) " to understand the configuration of VTY.

### Supervise and maintain VTY connection

Use the command *show line* to view VTY configuration.

Example of **VTY** configuration

Example of **TTY** configuration

Following configuration is to set bandwidth of terminal output and screen output lines of terminal. The user login at this port and the prompt *more* displayed per 40 lines. Line width limited in 132 characters, or go to newline:

```
[DEFAULT@Router /config/]#line
```

Key Word:

```
U(undo)          D(default)  Q(quit)
(00)aux          Auxiliary line
(01)console      Primary terminal line
(02)tty          Terminal controller
(03)vtty         Virtual terminal
```

Please Input the code of command to be excute(0-3): 2

Key Word:

```
Q(quit)
(00)<1-64>       First Line number
```

Please Input the code of command to be excute(0-0): 0

Please input a digital number:1 (input First Line number)

Key Word:

```
Q(quit)
(00)<2-64>       Last Line number
```

(01)<cr>

Please Input the code of command to be excute(0-1): 0

Please input a digital number:10 (input Last Line number)

Will you excute it? (Y/N):y

Key Word:

```
Q(quit)
```

.....

```
(35)where        display all outgoing telnet connection
```

```
(36)width        Set width of the display terminal
```

Please Input the code of command to be excute(0-36): 36

Key Word:

```
U(undo)          D(default)  Q(quit)
```

```

(00)<0-256>          Number of characters on a screen line(0 for no line wrap)
Please Input the code of command to be excute(0-0): 0
Please input a digital number:132 (input Number of characters)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(15)length          Set number of lines on a screen
(16)line            Configure a terminal line
.....
Please Input the code of command to be excute(0-36): 15
Key Word:
U(undo)            D(default)  Q(quit)
(00)<0-512>          Number of lines on screen (0 for no pausing)
Please Input the code of command to be excute(0-0): 0
Please input a digital number:40 (input Number of lines)
Will you excute it? (Y/N):y

```

Following configuration set s1/0 as TTY port.

```

Key Word:
Q(quit)
.....
(25)pdp              pdp configuration commands
(26)physical-layer  Configure physical layer parameters
.....
Please Input the code of command to be excute(0-34): 26
Key Word:
U(undo)              D(default)  Q(quit)
(00)flow-control    Flow control
(01)mode             Configure sync or async physical layer on serial interface
(02)sampling         set clock sampling mode
(03)speed            port speed
Please Input the code of command to be excute(0-3): 1
Key Word:
Q(quit)
(00)async            asynchronous mode
(01)sync             synchronous mode
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y

```

In this configuration, the straight back-to-back cable connected with s1/0 port. If the connection is remote access through Modem, *line dial* should be configured before the command *config-async mode interactive*.

### Example of VTY configuration

All the limitation of VTY screen output lines will be canceled by following configuration, prompt *more* will disappear.

```
[DEFAULT@Router /config/]#line
```

```

Key Word:
U(undo)  D(default)  Q(quit)
(00)aux              Auxiliary line

```

(01)console Primary terminal line  
 (02)tty Terminal controller  
 (03)vtty Virtual terminal

Please Input the code of command to be excute(0-3): **3**

Key Word:

Q(quit)

(00)<0-63> First Line number

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**0** ( input First Line number )

Key Word:

Q(quit)

(00)<1-63> Last Line number

(01)<cr>

Please Input the code of command to be excute(0-1): **0**

Please input a digital number:**63** ( input Last Line numbe )

Will you excute it? (Y/N):**y**

Key Word:

Q(quit)

.....

(15)length Set number of lines on a screen

(16)line Configure a terminal line

.....

Please Input the code of command to be excute(0-36): **15**

Key Word:

U(undo) D(default) Q(quit)

(00)<0-512> Number of lines on screen (0 for no pausing)

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**0** ( input Number of lines )

Will you excute it? (Y/N):**y**

### 3.15 configuring RMON

this chapter describes how to configure the RMON monitoring function on the D-link router.

Configure RMON alarm function

User can configure the RMON alarm function through the command line or SNMP network management application. If you configure it through the SNMP network management application, you should also configure the SNMP of router.

After enabling the alarm function, the device can monitoring some statistics of the system. The steps of configuring RMON alarm function is listed below:

step	command	function
1 .	<b>cd config</b>	Enter the global configurative mode

2 .	<b>rmon alarm</b> <i>index variable interval {absolute   delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [owner string]</i>	Add a RMON alarm item 1. ● <b>index</b> is the index of the items , range from 1 to 65535 2. ● <b>variable</b> --the object under monitoring of the MIB It must be a useful MIB object of the system, and only those objects with the types of INTEGER、Counter、 Gauge or TimeTicks can be detected. 3. ● <b>interval</b> is the time interval of sample, count in seconds. Its range is 1~4294967295 4. ● <b>absolute</b> is used to monitor the value of MIB object directly;delta is used to monitor the change of MIB-object value between two sample. 5. ● <b>value</b> is used to remark the limitation of creating an alarm, the corresponding eventnumber represent the index of events which will occur when the limitation is meet. 6. ● <b>owner string</b> can be used to describe some descriptive message of the alarm
3 .	<b>cd..</b>	Back to management mode
4 .	<b>write</b>	Save the configuration

[DEFAULT@Router /config/#**rmon**

Key Word:

U(undo) D(default) Q(quit)

(00)alarm Configure an RMON alarm

(01)event Configure an RMON event

Please Input the code of command to be excute(0-1): **0**

Key Word:

Q(quit)

(00)<1-65535> alarm number

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**100** (input alarm number)

Key Word:

Q(quit)

(00)WORD MIB object to monitor

Please Input the code of command to be excute(0-0): **0**

Please input a string:**abc** (input MIB object)

Key Word:

Q(quit)

(00)<1-4294967295> Sample interval

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**500** (input interval)

Key Word:

Q(quit)

(00)absolute Test each sample directly

(01)delta Test delta between samples

Please Input the code of command to be excute(0-1): **0**

Key Word:

Q(quit)

(00)rising-threshold Configure the rising threshold

Please Input the code of command to be excute(0-0): **0**

Key Word:

```

Q(quit)
(00)<-2147483648-2147483647>                rising threshold value
Please Input the code of command to be excute(0-0): 0
Please input a string:10000 ( input rising threshold value )
Key Word:
Q(quit)
(00)falling-threshold                      Configure the falling threshold
(01)<1-65535>                               Event to fire on rising threshold crossing
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00)<-2147483648-2147483647>                falling threshold value
Please Input the code of command to be excute(0-0): 0
Please input a string:100000 ( input falling threshold value )
Key Word:
Q(quit)
(00)<1-65535>                               Event to fire on falling threshold crossing
(01)owner                                  Specify an owner for the alarm
(02)<CR>
Please Input the code of command to be excute(0-2): 1
Key Word:
Q(quit)
(00)WORD                                   Alarm owner
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom ( input alarm owner )
Will you excute it? (Y/N):y
    
```

After configuring an item of alarm, device will get the oid value designated by variable every interval seconds, and compare the value with former one according to the alarm type(absolute or delta), if the current value is larger and exceed the limitation designated by the rising-threshold, the event whose index is eventnumber will be induced. ( if the eventnumber is 0 or the event table doesn't has an event whose index is eventnumber, the event will not be induced ) .vice versa ; if the oid designated by variable can not be get, the alarm table status of this line will be set as invalid. When the command "rmon alarm" is used many times to configure the same index of alarm item, only the parameters of last time is available. You can use the command "no rmon alarm *index*" to delete the alarm table whose index is *index*.

## Configuring the RMON event function

The steps of configuring the RMON event are listed below:

step	command	function
1 .	cd config	Enter the global configurative mode

2 .	<b>rmon event index</b> [description string] [log] [owner string] [trap community]	Add a RMON event table 7. ● <i>index</i> is the index of the items , its range is 1~65535 8. ● description is the descriptive information of the event 9. ● log means that a log message will be added to the log table whenever the event is induced. 10. ● trap means that a trap is generated when the event is induced, community is the group name. 11. ● owner string can be used to describe some descriptive message of the event.
3 .	<b>cd..</b>	Back to management mode
4 .	<b>write</b>	Save the configuration

[DEFAULT@Router /config/]#**rmon**

Key Word:

U(undo) D(default) Q(quit)  
(00)alarm Configure an RMON alarm  
(01)event Configure an RMON event

Please Input the code of command to be excute(0-1): **1**

Key Word:

Q(quit)  
(00)<1-65535> event number

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**10** (input event number)

Key Word:

Q(quit)  
(00)description Specify a description of the event  
(01)log Generate RMON log when the event fires  
.....

Please Input the code of command to be excute(0-4): **0**

Key Word:

Q(quit)  
(00)WORD Event description

Please Input the code of command to be excute(0-0): **0**

Please input a string:**fire** ( input Event description )

Key Word:

Q(quit)  
(00)log Generate RMON log when the event fires  
(01)trap Generate SNMP trap when the event fires  
.....

Please Input the code of command to be excute(0-3): **0**

Key Word:

Q(quit)  
(00)trap Generate SNMP trap when the event fires  
(01)owner Specify an owner for the event  
(02)<CR>

Please Input the code of command to be excute(0-2): **1**

Key Word:

Q(quit)

```
(00)WORD                                     Event owner
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom ( input Event owner )
Key Word:
Q(quit)
(00)trap                                     Generate SNMP trap when the event fires
(01)<CR>
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y
```

After your configuring the RMON event, when the RMON alarm is induced, the evenLastTimeSent region of the event item will be updated as the current sysUpTime firstly. If the event is configured with log attribute, a message will be added into the log table; If the event is configured with trap attribute, then a trap will be send while the group name is community. When the command “rmon event” is used many times to configure the same index of event item, only the parameters of last time is available. You can use the command “no rmon event index” to delete the event table whose index is *index*.

## Configuring collection function of the RMON

RMON collection group is used to monitoring the statistic information of each port. The configuration steps of RMON collection function are given below:

step	command	function
1 .	<b>cd config</b>	Enter the global configurative mode
2 .	<b>interface iftype ifid</b>	Enter the interface configurative mode 12. ● iftype is the type of the interface 13. ● ifid is ID of the interface
3 .	<b>rmon collection stat index</b> [owner string]	Enable the collection function of the interface 1. ● <i>index</i> is index of the collection items 2. ● owner string is used to describe some descriptive message of the collection items
4 .	<b>cd..</b>	Back to global configurative mode
5 .	<b>cd..</b>	Back to management mode
6 .	<b>write</b>	Save the configuration

```
[DEFAULT@Router /E1/1/]#rmon
```

```
Key Word:
U(undo) D(default) Q(quit)
(00)collection                               Configure Remote Monitoring Collection on an interface
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)history                                   Configure history
(01)stats                                     Configure statistics
Please Input the code of command to be excute(0-1): 0
Key Word:
```

```

Q(quit)
(00)<1-65535>                               Set RMON statistics control index
Please Input the code of command to be excute(0-0): 0
Please input a string:100 (input index number)
Key Word:
Q(quit)
(00)owner                                   Set the owner of this RMON collection
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom(input owner name)
Key Word:
Q(quit)
(00)<cr>
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y

```

When the command “rmon collection stat” is used many times to configure the same index of collection item, only the parameters of last time is available. You can use the command “no rmon collection stats index ” to delete the collection item whose index is *index*.

## Configuring the RMON history function

RMON history function is used to collect the statistic information of a port in various times. The steps of configuring the collection history are listed below:

step	command	function
1 .	<b>cd config</b>	Enter the global configurative mode
2 .	<b>interface iftype ifid</b>	Enter the interface configurative mode 14. ● iftype is type of the interface 15. ● ifid is ID of the interface
3 .	<b>rmon collection history index</b> [buckets bucket-number] [interval second] [owner owner-name]	Enable the RMON collection history function of the interface: 3. ● index is the <i>index</i> of history items 4. ● In all the statistics collected by the collection history function, item of the nearest bucket-number must be saved. You can get these statistics by browsing the Ethernet history record table. The default item number is 50. 5. ● second is the time interval between every two statistics acquisition. The default interval is 1800 seconds(halfhour) 6. ● owner string is used to describe some descriptive message of the collection history table
4 .	<b>cd..</b>	Back to the global configurative mode
5 .	<b>cd..</b>	Back to the management mode
6 .	<b>write</b>	Save the configuration

```
[DEFAULT@Router /E1/1/#rmon
```

Key Word:

```
U(undo)  D(default)          Q(quit)
```

```
(00)collection
```

Configure Remote Monitoring Collection on an interface

Please Input the code of command to be excute(0-0): **0**  
 Key Word:  
 Q(quit)  
 (00)history Configure history  
 (01)stats Configure statistics  
 Please Input the code of command to be excute(0-1): **1**  
 Key Word:  
 Q(quit)  
 (00)<1-65535> Set RMON history control index  
 Please Input the code of command to be excute(0-0): **0**  
 Please input a string:**100** (input index number)  
 Key Word:  
 Q(quit)  
 (00)buckets Requested buckets of intervals. Default is 50 buckets  
 (01)interval Interval to sample data for each bucket. Default is 1800  
 seconds  
 (02)owner Set the owner of this RMON collection  
 (03)<CR>  
 Please Input the code of command to be excute(0-3): **0**  
 Key Word:  
 Q(quit)  
 (00)<1-65535> Requested buckets of intervals  
 Please Input the code of command to be excute(0-0): **0**  
 Please input a string:**500** (input buckets of intervals )  
 Key Word:  
 Q(quit)  
 (00)interval Interval to sample data for each bucket. Default is 1800  
 seconds  
 (01)owner Set the owner of this RMON collection  
 (02)<CR>  
 Please Input the code of command to be excute(0-2): **0**  
 Key Word:  
 Q(quit)  
 (00)<1-3600> Interval in seconds to sample data for each bucket  
 Please Input the code of command to be exc ute(0-0): **0**  
 Please input a string:**100** (input value of Interval )  
 Key Word:  
 Q(quit)  
 (00)owner Set the owner of this RMON collection  
 (01)<CR>  
 Please Input the code of command to be excute(0-2): **0**  
 Key Word:  
 Q(quit)  
 (00)WORD RMON collection owner  
 Please Input the code of command to be excute(0-0): **0**  
 Please input a string:**bdcom** (input owner name )  
 Key Word:  
 Q(quit)  
 (00)<CR>

Please Input the code of command to be excute(0-0): **0**

Will you excute it? (Y/N):y

After being added a history table, the device will get a collection from the designated interface every *second* seconds and add the result as an item to the Ethernet history record table. When the command “rmon collection history index ” is used many times to configure an item with the same index, only the parameters of last time is available; you can use the command “ no rmon history index ” to delete the history item whose index is *index*. Note that it will occupy system resources if the bucket-number is too large or the interval second is two small.

## Display the RMON configuration

You can use the command “show” to display the RMON configuration of the router:

command	Function
<b>show rmon [alarm] [event] [statistics] [history]</b>	Display the configurative information of RMON <ul style="list-style-type: none"> <li>• ● alarm means that it will show the alarm items</li> <li>• ● event means that it will show the event items and items included in the log table which is created because of the event being induced.</li> <li>• ● statistics means that it will show the statistic items and the statistics acquired from the interface.</li> <li>• ● history means that it will show the history items and the statistics acquired from the interface during some given time intervals.</li> </ul>

- [DEFAULT@Router /config/#]show
- Key Word:
- U(undo) D(default) Q(quit)
- .....
- (34)rmon rmon statistics
- (35)route-map Information of route-map
- .....
- Please Input the code of command to be excute(0-50): **34**
- Key Word:
- Q(quit)
- (00)alarm Display the RMON alarm table
- (01)history Display the RMON history table
- (02)event Display the RMON event table
- (03)statistics Display the RMON statistics table
- (04)<cr>
- Please Input the code of command to be excute(0-4): **3**
- Key Word:
- Q(quit)
- (00)alarm Display the RMON alarm table
- (01)history Display the RMON history table
- (02)event Display the RMON event table
- (03)<cr>
- Please Input the code of command to be excute(0-3): **3**
- Will you excute it? (Y/N):y
- 
-

## 4. WANs Configuration

In this section, we will introduce the configuring method and process that of the correlative protocol of WAN. In addition, the configuring example will be provided to you for practice. The protocols of WAN that introduced in this section include: FR, X.25, PPP, PPPOE, SLIP, HDLC, LLC2 etc. You can straight enter the next index to search the content that you interested.

### 4.1 Overview

D-Link Router provides wide-range capacity of network that widely adapt to various environment of network.

#### 4.1.1 Destination of File

in this section we will introduce some general instruction of protocol component configuring as below:  
This section includes some brief description of technology. Please see the correlative chapters to obtain detailed information of configuration.

#### 4.1.2 Frame Relay (FR)

D-Link frame relay implements currently supported IP route and individual line.

Frame relay softwares provide following capabilities:

- Support three kinds implementing specifications that generally accepted by frame relay of local management interface (LMI).
  - The connecting specification of frame relay interface that assigned by Northern Telecom, Digital Equipment Corporation, StrataCom, and D-Link Systems.
  - T1.617 accessories D, the signal specification of frame relay that adopted by ANSI.
  - Q.933 accessories A, the signal specification of frame relay that adopted by telecommunication standard department of Internation Telecommunication Union (ITU-T).
- Accord with ITU-T I-series recommended 122, “attached packet mode provides service framework”
  - T1.618, the encapsulating specification of frame relay that adopted by ANSI.
  - Q.922 accessories A, the encapsulating specification of frame relay that adopted by ITU - T.
- Accord with RFC 2427 Internet engineering task Force (IETF) encapsulated except bridge.
- Support following keepalive mechanism, multicast group, status message:
  - Keepalive mechanism provides information exchange between network service and Exchange that varify the fluidness of data.
  - Multicast mechanism provides local Data Link Connection Identifier (DLCI) and multicast DLCI. The feature is special for implement the connecting specification of frame relay.
  - Status mechanism provides the status report of DLCI running that Exchange known.
- Support the reverse ARP protocol that described by RFC1293. It allowed the Router that running the frame relay protocol to detect the protocol address of end-to-end equipment with virtual circuit.
- Support the exchange of frame relay, the exchanging of data packet base on DLCI (medium accessing control address that correspond with frame relay). In the frame relay network, Router can be configured as mixed DTE Exchange or simple frame relay DCE accessing node. Following configurations are allowed by implementation of D-Link frame relay exchanging:
  - Exchanging in IP channel
  - Network - network interface (NNI) to other frame relay Exchange
  - Local serial - serial exchange

The frame relay exchange will be used while the entire flow that received by a DLCI can be sent to a similar next-skip address by another DLCI. In this condition, it is no need to examine the frame one by one for confirm the target address, and thereby reduce the load of Router.

### 4.1.3 LAPB and X.25

X.25 is one of a group of specifications published by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T); these specifications are international standards that are formally called *Recommendations*. The ITU-T Recommendation X.25 defines how connections between data terminal equipment (DTE) and data communications equipment (DCE) are maintained for remote terminal access and computer communications. The X.25 specification defines protocols for two layers of the OSI reference model. The data link layer protocol defined is LAPB. The network layer is sometimes called the packet level protocol (PLP), but is commonly (although less correctly) referred to as "the X.25 protocol."

The ITU-T updates its Recommendations periodically. The specifications dated 1980 and 1984 are the most common versions currently in use. Additionally, the International Standards Organization (ISO) has published ISO 7776:1986 as an equivalent to the LAPB standard, and ISO 8208:1989 as an equivalent to the ITU-T 1984 X.25 Recommendation packet layer. D-Link X.25 software follows the ITU-T 1984 X.25 Recommendation, except for its Defense Data Network (DDN) and Blacker Front End (BFE) operation, which follow the ITU-T 1980 X.25 Recommendation.

**Note** The ITU-T carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT). The 1988 X.25 standard was the last published as a CCITT Recommendation. The first ITU-T Recommendation is the 1993 revision.

In addition to providing remote terminal access, our X.25 software provides transport for LAN protocols—IP transmission.

Briefly, the D-Link X.25 software provides the following capabilities:

- LAPB datagram transport--LAPB is a protocol that operates at Level 2 (the data link layer) of the OSI reference model. It offers a reliable connection service for exchanging data (in units called frames) with one other host.
- X.25 datagram transport--X.25 can establish connections with multiple hosts; these connections are called virtual circuits. Protocol datagram (IP) is encapsulated inside packets on an X.25 virtual circuit. Mappings between a host's X.25 address and its datagram protocol addresses allow these datagrams to be routed through an X.25 network, thereby allowing an X.25 public data network (PDN) to transport LAN protocols.
- X.25 switch--X.25 calls can be routed based on their X.25 addresses either between serial interfaces on the same router to another router.
- PAD--User sessions can be carried across an X.25 network using the Packet Assembly and Disassembly (PAD) protocols defined by the ITU-T Recommendations X.3 and X.29.

D-Link X.25 implementation does not support fast switching.

### 4.1.4 HDLC

The High Level Data Link Control (HDLC) protocol is based on IBM's SNA (System Network Architecture) SDLC (Synchronous Data Link Control) protocol. IBM submitted SDLC to ANSI and ISO after development completed and the protocol separate into U.S. standard and international standard. ANSI modified the protocol into ADCCP (Advanced Data Communication Control Procedure); ISO modified the protocol into HDLC (Synchronous Data Link Control). CCITT then adopted and modified HDLC into Link Access Procedure (LAP) and subsequently become a part of X.25 interface standard. HDLC is bit-oriented protocol that ensures the transparent of data by bit filling.

HDLC is a protocol of data packet that defined a link encapsulation of IP packet on synchronous line and runTCP/IP on point-to-point serial line.

Usually, HDLC is use for DDN line with the feature of simplness and high efficiency.

### 4.1.5 SLIP

- ◆ The point-to-point data link layer protocol(such as SLIP, PPP) is needed for either the router-router leased line connection, or dialup host-router connection, to complete encapsulation of frame, error control, etc.
- ◆ SLIP is a data packet protocol, which defines series of characters to encapsulate the IP packet on serial line. For point-to-point line, use TCP/IP.
- ◆ SLIP implementation follow RFC 1055 and supports RFC 1144 suggested TCP/IP header compression. It is also supports various connections of network equipments and hosts through SLIP.

### 4.1.6 PPP

PPP provides the transmission of multiprotocol datagram on point-to-point link. D-Link Router mainly implemented following functions:

- . Follow RFC1661 and support Link Control Protocol to build, configure and test the link of data.
- . Follow RFC1662 and support the encapsulation of IP and other upper protocols on PPP that implement the IPCP of Network Control Protocol (NCP).
- . Follow RFC1334 and support two universal authenticating protocols that include PAP and CHAP.
- . Follow RFC1144 and support header compression of TCP/IP to improve the available data throughout.
- . Provide widely option control that adapts the situation in much more as possible and supports various connections of network equipment and host through the PPP protocol.
- . Support synchronous and asynchronous PPP protocol.
- . Support the option of multi-link to implement multi-link binding.
- . Support callback that provides higher security.
- . D-Link Router supports RADIUS protocol while use as dial-up server for authentication, authorization and accounting of user's identity. User info is saved in a host. The host and Router exchange the messages through RADIUS protocol.

## 4.2 Frame Relay Configuration Task List

### 4.2.1 Configuring Frame Relay

This chapter describes how to configuring Frame Relay on the router. For a complete description of the commands mentioned in this chapter, refer to the "Frame Relay Commands" chapter in the *Router Products Command Reference* publication.

### 4.2.2 Frame Relay Hardware Configurations

One of the following hardware configurations is possible for Frame Relay connections:

- Routers can connect directly to the Frame Relay switch.
- Routers can connect directly to a Channel Service Unit/Digital Service Unit (CSU/DSU) first, and the CSU/DSU connects to a remote Frame Relay switch.

---

**Note** Router can connect to a Frame Relay switch through a direct connection and others through connections via CSU/DSUs. However, a single router interface configured for Frame Relay can be only one or the other.

---

- ◆ The CSU/DSU converts V.35 or RS-449 signals to the properly coded E1/T1 transmission signal. Figure 1 illustrates the connections between the different components.

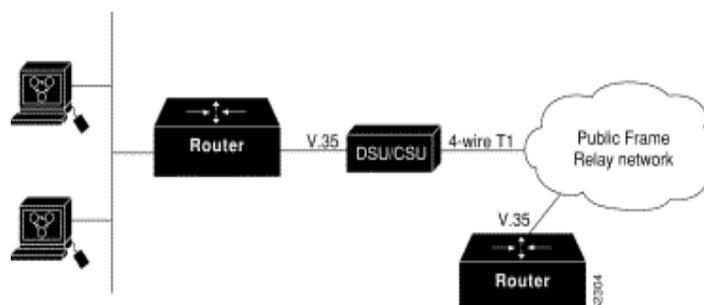


Figure 1: Typical Frame Relay Configuration

- ◆ The Frame Relay interface actually consists of one physical connection between the network server and the switch that provides the service. This single physical connection provides direct connectivity to each device on a network

### 4.2.3 Frame Relay Configuration Task

There are required, basic steps you must follow to enable Frame Relay for your network. In addition, you can customize Frame Relay for your particular network needs and monitor Frame Relay connections. The following sections outline these tasks.

Required configuration:

- ? Encapsulate Frame Relay on interface
- ? Configure Dynamic or Static Address Mapping

Following are optional configurations. These configurations can be modified by the requirement of application:

- ? Configure LMI
- ? Customerize configuration of network
- ? Monitor and maintain the Frame Relay connection

See the "Frame Relay Configuration Example" section at the end of this chapter for ideas of how to configure Frame Relay. See the "WAN Commands" chapter for information about the Frame Relay commands.

### 4.2.4 Enable Frame Relay Encapsulation on interface

To set Frame Relay encapsulation, perform the following tasks beginning in interface configuration mode:

Step	Command	Task
1	<b>interface</b> <i>type number</i>	Specify the interface, and enter interface configuration mode.
2	<b>Encapsulation(undo) frame-relay</b>	Enable Frame Relay and specify the encapsulation method. Command <i>no</i> is use for delete ports, which include configuration of subinterface Frame Relay encapsulating protocol.

```
[DEFAULT@Router /config/#interface
```

Key Word:

```
U(undo)  D(default)          Q(quit)
(00)FastEthernet          FastEthernet interface
(01)Ethernet              Ethernet interface
(02)Serial                 Serial interface
```

.....

```
Please Input the code of command to be excute(0-10): 2
```

```
Please input a interface names:s1/0
```

```
Will you excute it? (Y/N):y
```

Key Word:

```
Q(quit)
```

.....

```
(10)dsr-ignore            ignore dsr signal
(11)encapsulation         Set encapsulation type for an interface
```

.....

```
Please Input the code of command to be excute(0-34): 11
```

Key Word:

```
U(undo)  D(default)          Q(quit)
(00)frame-relay            Frame Relay Protocol
(01)hdlc                  HDLC Protocol
```

.....

```
Please Input the code of command to be excute(0-4): 0
```

Will you excute it? (Y/N):y

**Note:** There is two kinds of encapsulation of Cisco® router, the default Cisco® mode and the IETF(RFC 1490) mode. D-Link Router is able to automatic identify and dynamic adapt these two kinds of encapsulations.

#### 4.2.5 Configuring Dynamic or Static Address Mapping

- ◆ Dynamic address mapping uses Frame Relay Inverse ARP to request the next-hop protocol address for a specific connection, given its known DLCI. Responses to Inverse ARP requests are entered in an address-to-DLCI mapping table on the router; the table is then used to supply the next-hop protocol address or the DLCI for outgoing traffic.
- ◆ Inverse ARP is enabled by default for all protocols it supports. You can explicitly enable Inverse ARP if the protocol is supported on the other end of the connection. See the "Disable or Reenable Frame Relay Inverse ARP" section later in this chapter for more information.

#### 4.2.6 Configure Dynamic Mapping

Inverse ARP is opened to all protocols of all enabled network interfaces by default. Certainly, if the physical interface is disabled, the data packet cannot be transmitted and all Inverse ARP are unavailable. Because Inverse ARP is enabled by default for all protocols that it supports, no additional command is required to configure dynamic mapping on an interface.

#### 4.2.7 Configure Static Mapping

- ◆ A static map links a specified next-hop protocol address to a specified DLCI. Static mapping removes the need for Inverse ARP requests; when you supply a static map, Inverse ARP is automatically disabled for the specified protocol on the specified DLCI.
- ◆ You must configure static mapping if the router at the other end does not support Inverse ARP of Frame Relay.

To configure static mapping, perform the following *map* command in interface configuration mode:

Command	Task
<b>frame-relay (undo) map ip-address pvc dlc</b> <b>[broadcast]</b>	[Delete/Specify] the mapping between a next-hop protocol address and the DLCI.

Key Word:

Q(quit)

.....

(15)frame-relay Set parameters for Framerelay

(16)help Description of the interactive help system

.....

Please Input the code of command to be excute(0-32): **15**

Key Word:

U(undo) D(default) Q(quit)

.....

(04)local-dlci Set local DLCI parameters

(05)map Set map table for Framerelay

.....

Please Input the code of command to be excute(0-10): **5**

Key Word:

Q(quit)

(00)A.B.C.D IP address

Please Input the code of command to be excute(0-0): **0**

Please input a IP Address:**192.168.0.1** ( input ip address )

Key Word:

```

Q(quit)
(00)pvc                                PVC type
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)<16-1007>                          DLCI number
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:100 ( input pvc number )
Key Word:
Q(quit)
(00)broadcast                          Broadcasts should be forwarded to this address
(01)<cr>
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00)<cr>
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y
    
```

- ◆ You can be greatly simplifying the configuration for the Open Shortest Path First (OSPF) protocol by adding the optional **broadcast** keyword when doing this task.
- ◆ See the “Static Frame Relay Configuration Example” at the end of this chapter for more information about examples of static Frame Relay configuration.

#### 4.2.8 Straight configure the LMI

The Frame Relay software supports the industry-accepted standards of the Local Management Interface (LMI). To configure the LMI, complete the steps in the following sections. The step in the first is required.

#### 4.2.9 Set the LMI Type

- ◆ If the router is attached to a public data network (PDN), the LMI type must match the type used on the public network. Otherwise, you can select an LMI type to suit the needs of your private Frame Relay network.
- ◆ You can set following three types of LMIs on router: ANSI T1.617 Annex D, Group of Four Rev. #1, and ITU-T Q.933 Annex A. Of course, the LMI can be setted as *none*. To do so, perform the following command in interface configuration mode:

Setp	Command	Task
1	<b>Frame-relay (undo) lmi-type {ansi   bcisco   q933a }</b>	Set the LMI type, command no is use for restore the default configuration of LMI type
2	<b>exit</b>	Quit the configuration mode
3	<b>write</b>	Write the configuration

Key Word:

```

Q(quit)
.....
(15)frame-relay                        Set parameters for Framerelay
(16)help                               Description of the interactive help system
.....
Please Input the code of command to be excute(0-32): 15
Key Word:
    
```

U(undo) D(default) Q(quit)  
 (00)cir Set committed information rate  
 (01)intf-type Set interface mode for Frame Relay(DTE/DCE/NNI)  
 (02)inverse-arp Enable/disable Inverse ARP over Frame Relay  
 (03)lmi-type Set LMI type(q933a/ansi/lmi)

.....  
 Please Input the code of command to be excute(0-10): **3**

Key Word:  
 Q(quit)  
 (00)q933a LMI type is Q933A  
 (01)ansi LMI type is ANSI  
 (02)bcisco LMI type is compatible with others

Please Input the code of command to be excute(0-2): **1**

Will you excute it? (Y/N):**y**  
 Key Word:

Q(quit)  
 .....  
 (12)english help message in English  
 (13)exit exit / quit

.....  
 Please Input the code of command to be excute(0-32): **13**

Will you excute it? (Y/N):**y**  
 [DEFAULT@Router /config/]#**write**  
 Will you excute it? (Y/N):**y**

- ◆ After the Frame Relay encapsulating completed, the default LMI type is Autosense. This type is LMI of former 3000 series.
- ◆ For an example of how to set the LMI type, see the "Pure Frame Relay DCE Example" section later in this chapter.

#### 4.2.10 Set the Polling Intervals and Timer

You can set various optional counters, intervals, and thresholds to fine-tune the operation of your LMI DTE and DCE devices by performing the following commands:

Command	Task
<b>Frame-relay t391seconds</b>	Set a full status polling interval of link.
<b>Frame-relay t392 seconds</b>	Set the polling verification timer.
<b>Frame-relay n391number</b>	Set a full status polling interval timer
<b>Frame-relay n392 number</b>	Set the error threshold counter.
<b>Frame-relay n393 number</b>	Set the monitored event counter.

Key Word:  
 Q(quit)  
 .....  
 (14)fair-queue enable fair queue on interface  
 (15)frame-relay Set parameters for Framerelay

.....  
 Please Input the code of command to be excute(0-32): **15**

```

Key Word:
U(undo)  D(default)          Q(quit)
.....
(06)n391          Set LMI N391 counter
(07)n392          Set LMI N392 counter
(08)n393          Set LMI N393 counter
(09)t391          Set LMI T391 timer
(10)t392          Set LMI T392 timer
Please Input the code of command to be excute(0-10): 9 ( choose 6-10 for your demand )
Key Word:
Q(quit)
(00)<5-30>          LMI link integrity verification polling timer
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:10 ( input the time )
Will you excute it? (Y/N):y
    
```

See the correlative contents in "WAN Commands reference" chapter for details about commands used to set the polling and timing intervals.

#### 4.2.11 Configure Frame Relay Switching

Frame Relay switching is a means of switching packets based upon the DLCI, which can be looked upon as the Frame Relay equivalent of a MAC address. The switching is performed by configuring your router as a Frame Relay network. There are two parts to a Frame Relay network: a Frame Relay DTE (the router) and a Frame Relay DCE switch. Figure 2 illustrates this concept.

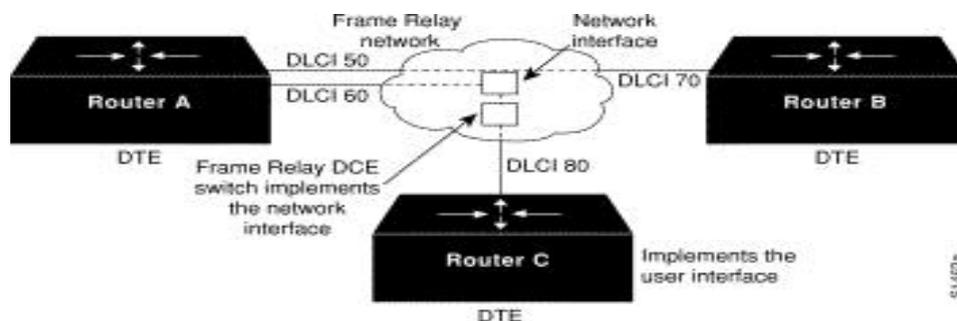


Figure 2: Frame Relay Switched Network

In Figure 2, Routers A, B, and C are Frame Relay DTEs connected to each other via a Frame Relay network. Our implementation of Frame Relay switching allows our routers to be used as depicted in this Frame Relay network.

Configure Frame Relay Switching by following steps:

- ? Configure a Frame Relay supported DTE Device, DCE Switch, or NNI interface
- ? Configure the static route

#### 4.2.12 Configure a Frame Relay supported DTE Device, DCE Switch, or NNI interface

You can configure the DTE device, DCE or NNI interface (DTE is the default.) that supported by Frame Relay switch. To do so, perform the following command in global configuration mode:

Command	Task
<b>Frame-relay intf-type [dce   dte   nni]</b>	Configure an interface type that supported by Frame Relay switch.

```

Key Word:
Q(quit)
    
```

```

.....
(14)fair-queue          enable fair queue on interface
(15)frame-relay         Set parameters for Framrelay
.....
Please Input the code of command to be excute(0-32): 15
Key Word:
U(undo)  D(default)      Q(quit)
(00)cir          Set committed information rate
(01)intf-type     Set interface mode for Frame Relay(DTE/DCE/NNI)

```

```

.....
Please Input the code of command to be excute(0-10): 1
Key Word:
Q(quit)
(00)dte          Set interface mode to FR DTE
(01)dce          Set interface mode to FR DCE
(02)nni          Set interface mode to FR NNI

```

Please Input the code of command to be excute(0-2): 1

Will you excute it? (Y/N):y

For an example of how to configure a DTE device or DCE switch, see the section "Hybrid DTE/DCE PVC Switching Example" later in this chapter.

For an example of how to configure NNI support, see the section "Example of configuration about DCE interface supported Frame Relay switch" later in this chapter.

#### 4.2.13 Specify the Static Route

Perform the following command in interface configuration mode to specify the route for PVC switching:

Command	Task
<b>Frswitch (undo) in-port in-dlci out-port out-dlci</b>	[Delete/Configure]static route of PVC

```

[DEFAULT@Router /config/]#frswitch
Key Word:
U(undo)  D(default)      Q(quit)
(00)Serial          Serial interface
Please Input the code of command to be excute(0-0): 0
Please input a interface name:s1/1 ( input the interface name )
Key Word:
Q(quit)
(00)nnnn          PVC number
Please Input the code of command to be excute(0-0):0
Please input a string:100 ( input the PVC number )
Key Word:
Q(quit)
(00)Serial          Serial interface
Please Input the code of command to be excute(0-0): 0
Please input a interface name:s1/2 ( input the interface name )
Key Word:
Q(quit)
(00)nnnn          PVC number
Please Input the code of command to be excute(0-0): 0

```

Please input a string:**200** ( input the PVC number )

Will you excute it? (Y/N):**y**

For an example of how to specify a static route, see the section "Example of configure Frame Relay switch" later in this chapter.

#### 4.2.14 Disable or Reenable Frame Relay Inverse ARP

Frame Relay Inverse ARP is a method of searching DLCI protocol address in Frame Relay networks.

Inverse ARP creates dynamic address mappings, as contrasted with the frame-relay map command, which build static mappings. See the section "Configure Dynamic or Static Address mapping" earlier in this chapter for more information.

Inverse ARP is enabled by default Disable or reenable Inverse ARP in the following conditions:

- ? Disable Inverse ARP for a selected protocol and DLCI pair when you know that the protocol is not supported on the other end of the connection.
- ? Reenable Inverse ARP for a protocol and DLCI pair if equipment change and the protocol is then supported on the other end of the connection.

To enable or disable Inverse ARP, perform the following command in interface configuration mode:

Command	Task
<b>frame-relay inverse-arp</b>	Enable Inverse ARP of Frame Relay.
<b>frame-relay (undo) inverse-arp</b>	Disable Inverse ARP of Frame Relay.

Key Word:

Q(quit)

.....

(14)fair-queue enable fair queue on interface

(15)frame-relay Set parameters for Framerelay

.....

Please Input the code of command to be excute(0-32): **15**

Key Word:

U(undo) D(default) Q(quit)

(00)cir Set committed information rate

(01)intf-type Set interface mode for Frame Relay(DTE/DCE/NNI)

(02)inverse-arp Enable/disable Inverse ARP over Frame Relay

.....

Please Input the code of command to be excute(0-10): **2**

Will you excute it? (Y/N):**y**

#### 4.2.15 Configure Frame Relay Subinterfaces

Please see the "Connect the Frame Relay Subinterface" for connect and define the frame relay subinterface. Perform the following configuring for difine the frame relay subinterface:

? Define Frame Relay Subinterface

? Specify the Subinterface Address

Please see the "Subinterface Configuration Example" at the end of this chapter for examples of define the subinterface configuration.

#### 4.2.16 Understand Frame Relay Subinterfaces

- ◆ Sub-interface supports multiple logic interface or network interconnection on a physical interface, that is, it can associated multiple logic interfaces with a physical interface. The logic ones share the parameters of physical interface though each has its parameters of data link layer and network layer of the ISO 7-layered architecture.
- ◆ Frame Relay subinterfaces provide a mechanism for supporting partially meshed Frame Relay networks. Most

protocols assume *transitivity* on a logical network; that is, if station A can talk to station B, and station B can talk to station C, then station A should be able to talk to station C directly. Transitivity is true on LANs, but not on Frame Relay networks unless A is directly connected to C.

- ◆ Configuring Frame Relay subinterfaces ensures that a *single physical interface* is treated as *multiple virtual interfaces*. This capability allows us to overcome split horizon rules. Packets received on one virtual interface can now be forwarded out another virtual interface, even if they are configured on the same physical interface.
- ◆ Sub-interfaces address the limitations of Frame Relay networks by providing a way to subdivide a partially meshed Frame Relay network into a number of smaller, fully meshed (or point-to-point) sub-networks. Each sub-network is assigned its own network number and appears to the protocols as if it is reachable through a separate interface.
- ◆ User can configure the following items on the WAN sub-interface with Frame Relay encapsulation:
  - DLCI or Frame Relay address mapping differ with original WAN interface
  - IP address in different networks with the original WAN interface

#### 4.2.17 Define Frame Relay Subinterfaces

To configure subinterfaces on a Frame Relay network, perform the following command in global configuration mode:

Step	Command	Task
1	<b>interface</b> <i>type number</i>	Specify an interface.
2	<b>encapsulation frame-relay</b>	Configure Frame Relay encapsulation on the serial interface.
3	<b>interface</b> <i>type number.subinterface-number</i> { <b>multipoint</b>   <b>point-to-point</b> }	Specify a subinterface.

```
[DEFAULT@Router /config/]#interface
```

```
Key Word:
```

```
U(undo)  D(default)          Q(quit)
(00)FastEthernet             FastEthernet interface
(01)Ethernet                 Ethernet interface
(02)Serial                   Serial interface
```

```
.....
```

```
Please Input the code of command to be excute(0-10): 2
```

```
Please input a interface name:s1/0 ( input the interface name )
```

```
Will you excute it? (Y/N):y
```

```
Key Word:
```

```
Q(quit)
.....
(11)encapsulation           Set encapsulation type for an interface
(12)english                 help message in English
```

```
.....
```

```
Please Input the code of command to be excute(0-32): 11
```

```
Key Word:
```

```
U(undo)  D(default)          Q(quit)
(00)frame-relay             Frame Relay Protocol
(01)hdlc                    HDLC Protocol
```

```
.....
```

```
Please Input the code of command to be excute(0-4): 0
```

```
Will you excute it? (Y/N):y
```

```
Key Word:
```

```
Q(quit)
```

```
.....
```

(17)history look up history  
 (18)interface interface configuration  
 .....

Please Input the code of command to be excute(0-32): **18**

Key Word:

U(undo) D(default) Q(quit)  
 (00)FastEthernet FastEthernet interface  
 (01)Ethernet Ethernet interface  
 (02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10): **2**

Please input a interface name:s**1/0.1** ( input the sub-interface name )

(00)multipoint -- multi-point sub-interface  
 (01)point-to-point -- point to point sub-interface

Please Input the code of command to be excute(0-1): **1**

Subinterfaces can be configured for multipoint or point-to-point communication. (There is no default.)

#### 4.2.18 Specify Subinterface Address

For frame relay subinterface, the particular subinterface DLCI value can be configured by set **frame-relay local-dlci** command if the main interface work in the DCE mode. The target end can be dynamic resolve through reverse ARP or static mapping by **map** command

#### 4.2.19 Configure DLCI

Use following command to configure DLCI value of subinterface:

Command	Purpose
<b>Frame-relay (undo) local-dlci</b> <i>dlci</i> [ <i>cir speed</i> ]	[delete/specify]DLCI of subinterface

Key Word:

Q(quit)  
 .....

(14)fair-queue enable fair queue on interface  
 (15)frame-relay Set parameters for Framerelay  
 .....

Please Input the code of command to be excute(0-32): **15**

Key Word:

U(undo) D(default) Q(quit)  
 .....

(03)lmi-type Set LMI type(q933a/ansi/lmi)  
 (04)local-dlci Set local DLCI parameters  
 .....

Please Input the code of command to be excute(0-10): **4**

Key Word:

Q(quit)  
 (00)<16-1007> Local DLCI

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:Please input a string:**100** ( input the DLCI number )

Key Word:

Q(quit)

```
(00)cir                               Set committed information rate
(01)<cr>
```

Please Input the code of command to be excute(0-0): 1

**Note: This command can use for both subinterface and main interface. Only one DLCI can be configured for point-to-point subinterface.**

#### 4.2.20 Configure Inverse ARP for Dynamic Address Mapping on Subinterfaces

- ◆ Dynamic address mapping uses Frame Relay Inverse ARP to request the next-hop protocol address for a specific connection, given a DLCI. Responses to Inverse ARP requests are entered in an address-to-DLCI mapping table on the router; the table is then used to supply the next-hop protocol address or the DLCI for outgoing traffic.
- ◆ Since the physical interface is now configured as multiple subinterfaces, you must provide information that distinguishes a subinterface from the physical interface. Inverse ARP must be enabled in main interface so that the interface can create Dynamic Address Mapping by Inverse ARP .
- ◆ To associate a subinterface with a specific DLCI, perform the following command:

Command	Task
<b>Frame-relay local-dlci</b> <i>dlci</i> [ <b>cir</b> <i>speed</i> ]	Specify DLCI for multipoint subinterface.

Refer to “configuring DLCI” of the former example.

#### 4.2.21 Configure Static Address Mapping for Subinterfaces

A static map links a specified next-hop protocol address to a specified DLCI.

To configure static mapping, perform one of the following tasks in interface configuration mode:

Command	Task
<b>Frame-relay (undo) map</b> <i>ipaddress</i> <b>pvc</b> <i>dlci</i> [ <b>broadcast</b> ]	[Delete/Create] Define the mapping between a next-hop protocol address and the DLCI

Please refer to the “configuring static address mapping” above.

**Note: only one static mapping can be configured for point-to-point interface.**

#### 4.2.22 Monitor and maintain the Frame Relay Connections

To monitor Frame Relay connections, perform the following command in configuration mode. For more detail, please refer to the “commands of configuring Frame-relay”

Command	Task
<b>show interface</b> <i>type number</i>	Display DLCI type and LMI type of Frame Relay.
<b>show frame-relay</b>	Display current Frame Relay Mapping.
<b>show frswitch</b>	Display the information of Frame Relay switch.

```
DEFAULT@Router /config/)#show
```

Key Word:

```
U(undo)  D(default)          Q(quit)
```

```
.....
```

```
(20)interface                interface status and configuration
```

```
(21)ip                       IP information
```

```
.....
```

Please Input the code of command to be excute(0-49): 20

Key Word:

Q(quit)

.....

(02)Serial                                Serial interface

(03)Async                                 Asynchronous interface

Please Input the code of command to be excute(0-3): **2**

Please input a interface name:**s1/0** ( input the interface name )

Will you excute it? (Y/N):**y**

If you want to show the message of frame-relay mapping or switching :

[DEFAULT@Router /config/#**show**

Key Word:

U(undo)    D(default)                    Q(quit)

.....

(16)frame-relay                         Display Frame Relay state

(17)frswitch                             Display Frame Relay switch state

.....

Please Input the code of command to be excute(0-49): **16** ( you can also choose 17 to show **也可选** the frame-relay switch )

Will you excute it? (Y/N):**y**

#### 4.2.23 Frame Relay Configuration Examples

This section provides examples of Frame Relay configurations. It includes the following sections:

#### 4.2.24 Encapsulation Examples

The first example that follows sets Frame Relay encapsulation at the interface.

```
encapsulation frame-relay
frame-relay map 131.108.123.2 pvc 48
frame-relay map 131.108.123.3 pvc 49 broadcast
```

#### 4.2.25 Static Address Mapping Examples

The following sections provide examples of how to configure static mapping.

```
Router 1
interface s1/0
ip address 131.108.64.2 255.255.255.0
encapsulation frame-relay
frame-relay intf-type dce
frame-relay local_dlci 43
frame-relay map 131.108.64.1 pvc 43
Router 2
interface s1/0
ip address 131.108.64.1 255.255.255.0
encapsulation frame-relay
frame-relay map 131.108.64.2 pvc 43
```

#### 4.2.26 Frame Relay Switching Examples

The following sections provide several examples of configuring one or more routers as Frame Relay switches:

##### PVC Switching Configuration Example

-- In this example, one router has two interfaces configured as DCEs; the router switches frames from the incoming

interface to the outgoing interface on the basis of the DLCI alone.

#### Pure Frame Relay DCE Example

-- In this example, a Frame Relay network is set up with two routers functioning as switches; standard NNI signaling is used between them.

#### Hybrid DTE/DCE PVC Switching Example

-- In this example, one router is configured with both DCE and DTE interfaces (a hybrid DTE/DCE Frame Relay switch). It can switch frames between two DCE ports and between a DCE port and a DTE port.

#### 4.2.27 PVC Switching Configuration Example

You can configure your router as a dedicated, DCE-only Frame Relay switch. Switching is based on DLCIs. The incoming DLCI is examined, and the outgoing interface and DLCI are determined. Switching takes place when the incoming DLCI in the packet is replaced by the outgoing DLCI, and the packet is sent out the outgoing interface.

In the following Figure 3, the router switches two PVCs between interface serial 1 and 2. Frames with DLCI 100 received on serial 1 will be transmitted with DLCI 200 on serial 2.

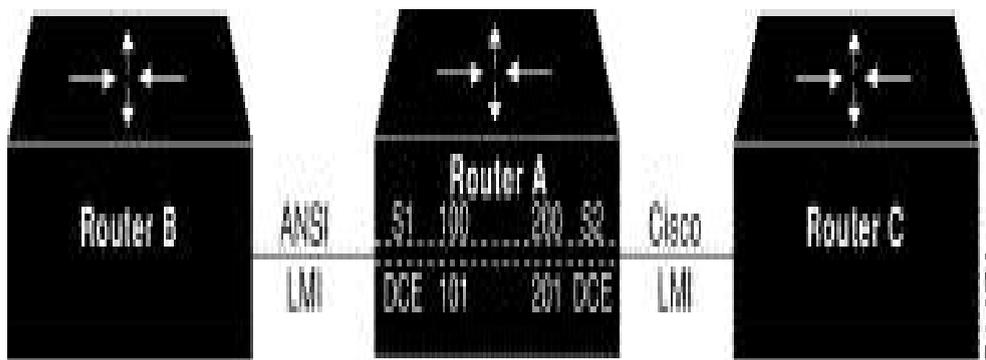


Figure 3: PVC Switching Configuration

#### Configuration of Router A

```
!
interface s1/1
encapsulation frame-relay
frame-relay lmi-type ansi
frame-relay intf-type dce
frame-relay local-dlci 100
!
interface s1/2
encapsulation frame-relay
frame-relay intf-type dce
frame-relay local-dlci 200
!
frswitch s1/1 100 s1/2 200
```

#### 4.2.28 Pure Frame Relay DCE Example

Using the PVC switching feature, it is possible to build an entire Frame Relay network using our routers. In the following Figure 4, Router A and Router C act as Frame Relay switches implementing a two-node network. The standard Network-to-Network Interface (NNI) signaling protocol is used between Router A and Router C.

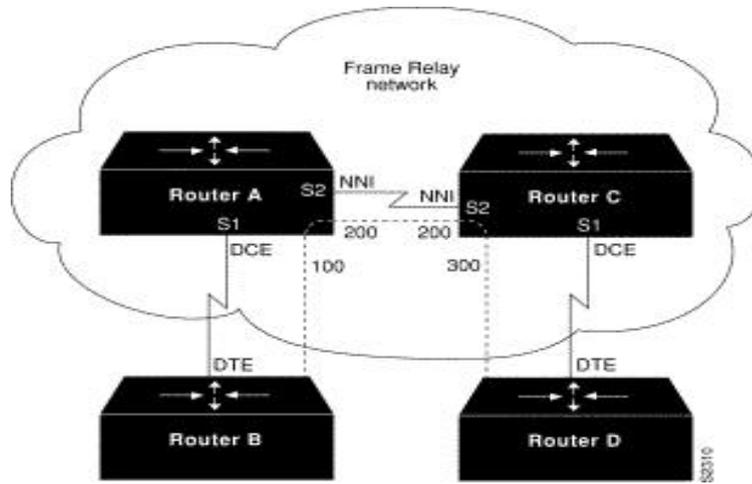


Figure 4: Frame Relay DCE Configuration

**Configuration of Router A**

!

```

interface s1/1
encapsulation frame-relay
frame-relay intf-type dce
frame-relay lmi-type ansi
frame-relay local-dlci 100
!
interface s1/2
encapsulation frame-relay
frame-relay intf-type nni
frame-relay lmi-type q933a
frame-relay local-dlci 200
!
frswitch s1/1 100 s1/2 200

```

**Configuration of Router C**

!

```

interface s1/1
encapsulation frame-relay
frame-relay intf-type dce
frame-relay lmi-type ansi
frame-relay local-dlci 300
!
interface s1/2
encapsulation frame-relay
frame-relay intf-type nni
frame-relay lmi-type q933a
frame-relay local-dlci 200
!
frswitch s1/1 300 s1/2 200

```

**4.2.29 Hybrid DTE/DCE PVC Switching Example**

Routers can also be configured as hybrid DTE/DCE Frame Relay switches, see Figure 5:

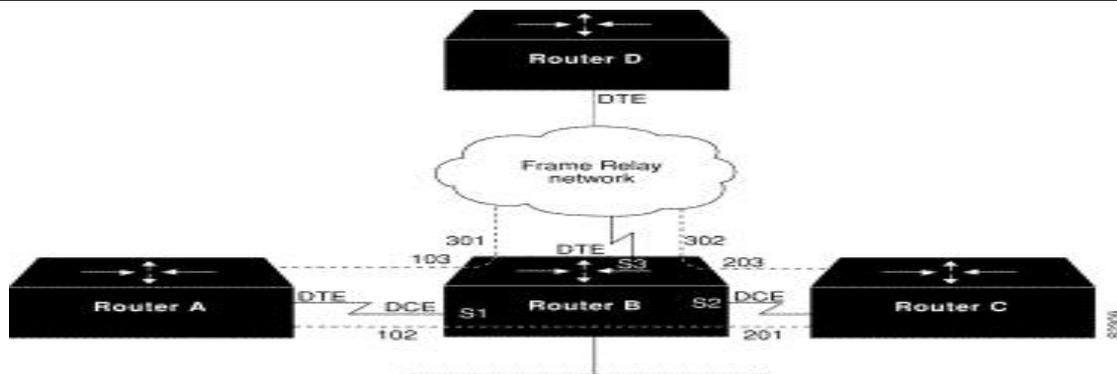


Figure 5: Hybrid DTE/DCE PVC Switching

In the following example, Router B acts as a hybrid DTE/DCE Frame Relay switch. It can switch frames between the two DCE ports and between a DCE port and a DTE port. Traffic from the Frame Relay network can also be terminated locally.

In the example, three PVCs are defined, as follows:

- Serial 1, DLCI 102 to serial 2, DLCI 201 DCE switching
- Serial 1, DLCI 103 to serial 3, DLCI 301 DCE/DTE switching
- Serial 2, DLCI 203 to serial 3, DLCI 302 DCE/DTE switching

DLCI 400 is also defined for locally terminated traffic.

#### Configuration of Router B

```
!
interface s1/1
encapsulation frame-relay
frame-relay intf-type dce
frame-relay local-dlci 102
frame-relay local-dlci 103
!
interface s1/2
encapsulation frame-relay
frame-relay intf-type dce
frame-relay local-dlci 201
frame-relay local-dlci 203
!
interface s1/3
ip address 131.108.111.231 255.255.0.0
encapsulation frame-relay
frame-relay lmi-type ansi
frame-relay map 131.108.111.4 pvc 400 broadcast
!
frswitch s1/1 102 s1/2 201
frswitch s1/1 103 s1/3 301
frswitch s1/2 203 s1/3 302
```

#### 4.2.30 Subinterface Examples

The following sections provide basic Frame Relay subinterface examples.

##### Basic Subinterface Examples

In the following example, subinterface 1 models a point-to-point subnet and subinterface 2 models a multipoint subnet.

```
interface s1/0
encapsulation frame-relay
```

```

frame-relay intf-type dce
interface s1/0.1 point-to-point
ip address 10.0.1.1 255.255.255.0
frame-relay local-dlci 20
frame-relay map 10.0.1.2 pvc 20
!
interface s1/0.2 multipoint
ip addr10.0.2.1 255.255.255.0
frame-relay local-dlci 20
frame-relay map 10.0.2.2 pvc 20

```

### Configure Frame Relay Subinterface with Dynamic Address Mapping

The following example configures two subinterfaces for dynamic address resolution. Each subinterface is provided with an individual protocol address and subnet mask.

#### framerelay

**local-dlci Command** specify DLCI for subinterface. Each subinterface acquired remote address by dynamic address resolution.

```

interface s1/0
ip (undo) address
encapsulation frame-relay
frame-relay inverse-arp
frame-relay lmi-type ansi
!
interface s1/0.103 multipoint
ip address 192.168.177.18 255.255.255.0
frame-relay local-dlci 300
!
interface s1/0.104 multipoint
ip addr192.168.178.18 255.255.255.0
frame-relay local-dlci 400

```

#### 4.3 X.25 Configuration Task List

- ◆ This chapter describes how to configure connections through Link Access Procedure, Balanced (LAPB) connections and X.25 networks. X.25 protocol is connection-oriented reliable data transmitting protocol, which includes the LAPB rules of OSI data link layer and X.25 rules of network layer. X.25 rules defines two types of hosts: DTE and DCE.
- ◆ The router using X.25 encapsulation can use as DTE or DCE equipment on protocol layer, that different from hardware DTE and DCE.
- ◆ To understand the complete description of the commands in this chapter, please see the “X.25 and LAPB command” chapter of *WAN Command Reference*. Use command index for other commands appeared in this chapter.

#### 4.3.1 Configure LAPB

X.25 Level 2 or LAPB operates at the data link layer of the OSI reference model. LAPB specifies methods for exchanging data (in units called *frames*), detecting out-of-sequence or missing frames, retransmitting frames, and acknowledging frames. Several protocol parameters can be modified to change LAPB protocol performance on a particular link. Because X.25 operates the Packet Level Protocol (PLP) on top of the LAPB protocol, these tasks apply to both X.25 links and LAPB links. The parameters and their default values are summarized in Table 5.



- LAPB T2—The value of T2 of DTE can be different from that of DCE, however, they should inform each other. If the T2 timer is expired, the DTE(or DCE) must send a confirmation frame to the DTE(or DCE) of the partner before the partner's T1 timer expired.

For leased-line circuits, the T1 timer setting is critical because the design of LAPB assumes that a frame has been lost if it is not acknowledged within period T1. The timer setting must be large enough to permit a maximum-sized frame to complete one round trip on the link. If the timer setting is too small, the software will poll before the acknowledgment frame can return, which may result in duplicated frames and severe protocol problems. If the timer setting is too large, the software waits longer than necessary before requesting an acknowledgment, which reduces bandwidth.

For the examples of configuring the LAPB T1 timer, refer to "typical LAPB configuration examples".

### X.25 configuration task list

To configure X.25, complete the tasks in one or more of the following sections, depending upon the X.25 application or task required for your network. The interface, datagram transport, and routing tasks are divided into sections based generally on how common the feature is and how often it is used. Those features and parameters that are relatively uncommon are found in the "Additional" sections. LAPB frame parameters can be modified to optimize X.25 operation, as described earlier in this chapter.

Default parameters are provided for X.25 operation; however, you can change the settings to meet the needs of your X.25 network or as defined by your X.25 service supplier. D-LINK also provides additional configuration settings to optimize your X.25 usage.

**Note** If you connect a router to an X.25 network, use the parameters set by your network administrator for the connection; these parameters will typically be those described in the "Configure an X.25 Interface" and "Modify LAPB Protocol Parameters" sections. Also, note that the X.25 Level 2 parameters described in the "Modify LAPB Protocol Parameters" section affect X.25 Level 3 operations.

See the end of this chapter for examples of configuring the X.25.

### Configure an X.25 interface

To configure an X.25 interface, perform the tasks in the following sections:

- encapsulate the X.25
- set the X.25 mode
- set the virtual circuit ranges
- set the X.121 address
- set the default flow control values

These tasks describe the parameters that are essential for correct X.25 behavior. The first task is required. The others might be required or optional, depending on what the router is expected to do and on the X.25 network.

### encapsulating the X.25 protocol

User must encapsulate the X.25 protocol in the interface configuration mode before configuring the X.25

command	Function
<b>encapsulation x25</b>	Encapsulate X.25

Key Word:

Q(quit)

.....

(11)encapsulation

Set encapsulation type for an interface

(12)english

help message in English

.....

Please Input the code of command to be excute(0-30): **11**

Key Word:

U(undo) D(default)

Q(quit)

.....

(03)sdlc

SDLC Protocol

(04)x25

X.25 Protocol





```

U(undo)   D(default)           Q(quit)
(00)address                               Set local X.121 address
(01)alias                               Set address alias for this port
.....
Please Input the code of command to be excute(0-26): 0
Key Word:
Q(quit)
(00)WORD                               Local X.121 address
Please Input the code of command to be excute(0-0): 0
Please input a string:123456 ( input the x121 address )

```

Will you excute it? (Y/N):y

For an example of configuring the X.25 interface address, see the section "Typical X.25 Configuration Example" later in this chapter.

### 4.3.2 Set default flow control values

Setting correct default flow control parameters of window size and packet size is essential for correct operation of the link because X.25 is a strongly flow controlled protocol. However, it is easy to overlook this task because many networks use standard default values. Mismatched default flow control values will cause X.25 local procedure errors, evidenced by Clear and Reset events.

To configure flow control parameters, complete the tasks in the following sections.

- set default window size
- set default packet size

To configure X.25 flow control values, perform the following commands in interface configuration mode:

command	function	range	default
<b>x25 psize</b> <i>size</i>	Set the packet size(Byte)	128,256,512,1024	128
<b>x25 wsize</b> <i>packets</i>	Set the window size	2- ( modulo-1 )	2

```

Key Word:
U(undo)           D(default)           Q(quit)
.....
(18)psize                               Set X.25 max packet size
.....
(25)wsize                               Set X.25 level 3 window size
(26)pad-access                               Accept only PAD connections from statically mapped X25 hosts
Please Input the code of command to be excute(0-26): 18 ( you can also choose 25 to set the wsize )
Key Word:
Q(quit)
(00)<128-1024>                               Maximum input packet size (power of 2)
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:512 ( input packet size )
Will you excute it? (Y/N):y

```

**Note** Because the X.25 protocol requires the DTE and DCE to have identical default maximum packet sizes and default window sizes, changes made to the window and packet sizes when the interface is up are held until the X.25 protocol restarts the packet service.

### Configure additional X.25 interface parameters

Some X.25 applications have less common or special needs. Several X.25 parameters are available to modify the X.25 protocol behavior for these applications.

To configure less common X.25 interface parameters for these special needs, perform the tasks in the following sections, as needed:

- set the X.25 level three timers
- set the X.25 address

#### 4.3.3 Set the X.25 level 3 timers

To set the retransmission timers, perform any of the following tasks in interface configuration mode

command	Task
<b>x25 t20 seconds</b>	Set DTE T20 reset request, default value=180sec
<b>x25 t23 seconds</b>	Set DTE T23 clear request, default value=180sec

Key Word:

Q(quit)

.....

(29)snmp                      Modify SNMP interface parameters

(30)x25                         Set parameters for X.25

Please Input the code of command to be excute(0-30): **30**

Key Word:

U(undo)    D(default)            Q(quit)

.....

(22)t20                         Set X.25 DTE Restart Request retransmission timer

(23)t23                         Set X.25 DTE Clear Request retransmission timer

.....

Please Input the code of command to be excute(0-26): **22** ( you can also choose 23 to set t23 )

Key Word:

Q(quit)

(00)<1-1000>                    X.25 DTE restart timer(second)

Please Input the code of command to be excute(0-0): **00**

Please input a digital number:Please input a string:**100** ( input DTE restart timer )

Will you excute it? (Y/N):**y**

For an example of setting the retransmission timers, see the section "DDN X.25 Configuration Example" later in this chapter.

#### 4.3.4 Set the X.25 address

When establishing SVCs, X.25 uses addresses in the form defined by the ITU-T *Recommendation X.121* (or simply an "X.121 address"). An X.121 address has from zero to 15 digits. Because of the importance of addressing to call setup, several interface addressing features are available for X.25.

To configure the X.25 address, perform the following tasks:

- understand the normal X.25 address
- configure an interface Alias address

##### Understand normal X.25 address

An X.25 interface's X.121 address is used when it is the source or destination of an X.25 call. The X.25 call setup procedure identifies both the calling (source) and the called (destination) X.121 addresses. When an interface is the source of a call, it encodes the interface X.121 address as the source address. An interface determines that it is the destination of a received call if the destination address matches the interface's address.

D-LINK's X.25 software can also route X.25 calls, which involves placing and accepting calls, but the router is neither the source nor the destination for these calls. Routing X.25 does not modify the source or destination addresses,





Ebackup means the address mapping is an enhance backup type.

**NOTE: Multi-protocol mapping, especially configured with broadcast, can cause particularly large communication load which need more queues, windows and virtue circuits. User can configure the OSPF through the command “broadcast”. Refer to the chapter “X.25 and LAPB commands” for the description of command “Map”.**

**Mapping the destination X.121 address to logic virtue interface**

This chapter illustrates how to make a remote PC access the local network through the X.25 network by configuring the router.

Firstly, the remote computer access the PSTN( or directly access X.25 ) network through normal dialing mode. The network supplier transfer the call to X.25 network through PAD( packet assembler/disassembler). If the local router is configured to map the destination X.121 address to the logic virtue interface, it will response the call and transfer the call to the PPP which will perform the authentication, registration, authorization and so on. The remote computer can access the local network

if it pass the authenticaiton.

Use the following command in the configuration mode:

Command	task
<b>Translate</b> (undo) <b>x25</b> <i>x121-address</i> <b>virtual-template</b> <i>virtual-template-interface-number</i>	add/delete a X.121 address mapping to virtue circuit

```
[DEFAULT@Router /config/]#t translate
(00)x25          Translate to X.25 encapsulation
(01)tcp          Translate packet between TCP and X.25
Please Input the code of command to be excute(0-1): 0
(00)WORD        X.121 address
Please Input the code of command to be excute(0-0): 0
Please input a string:12345678 (input the x121address )
(00)Virtual-template Virtual template interface
Please Input the code of command to be excute(0-0): 00
Please input a interface name:vt1 (input the virtual-temlate interface name)
Will you excute it? (Y/N):y
```

The basic configuration figure is giving below:

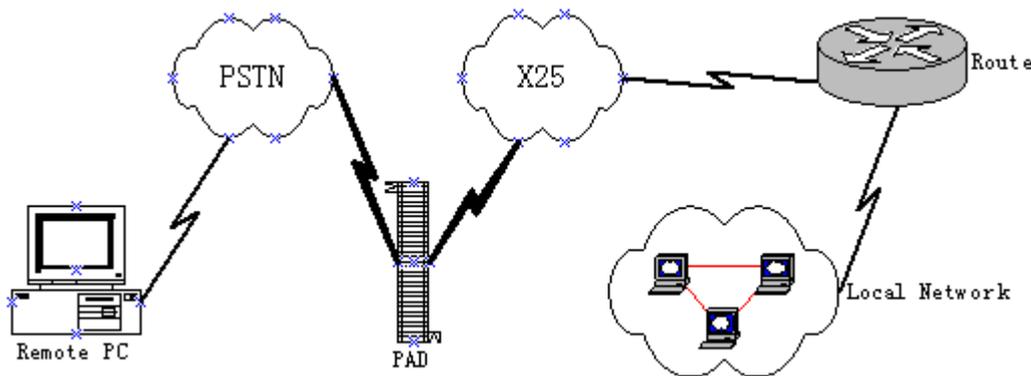


Figure 1 typical configuration of mapping the X.121address to virtue interface

**Configure additional X.25 routing features**

The software of D-LINK router has the capability of configuring additional X.25 routing features:

To configure the X.25 routing features, perform the tasks in the following sections:

- set the encapsulation for virtue circuit idle time
- set theX.25 negotiation parameters

### 4.3.6 set the encapsulation for virtue circuit idle time

The router will clear its switching virtue circuit after a idle period of time.

To set the idle time, use the following command in the interface configuration mode:

command	task
<b>x25 idle</b> <i>seconds</i>	Set the idle time for clearing the virtue circuit, range(0-2147483647),default 100 sec

Key Word:

U(undo) D(default) Q(quit)

.....

(29)snmp Modify SNMP interface parameters

(30)x25 Set parameters for X.25

Please Input the code of command to be excute(0-30): **30**

Key Word:

U(undo) D(default) Q(quit)

.....

(07)idle Set inactivity time before clearing SVC

(08)incallcheck Check calling address in incall packet or not

.....

Please Input the code of command to be excute(0-26): **7**

Key Word:

Q(quit)

(00)<0-2147483647> Idle time for X.25 SVC connection of IP keep alive(second)

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:Please input a string:**300** ( input the idle time )

Will you excute it? (Y/N):**y**

Refer to the "typical X.25 configuration examples" for the SVC idle time configuration examples.

### configure the X.25 negotiation parameters

X.25 software provides commands which support configuration of X.25 negotiation parameters and allow D bit settings,

To set supported X.25 negotiation parameters, use the command given below in interface configuration mode:

command	Task
<b>x25 (undo) dbit</b>	Set to use the D bit setting whether or not
<b>x25 (undo) nps</b>	enable/disable packet length negotiation
<b>x25 (undo) nws</b>	enable/disable packet window size negotiation
<b>x25 (undo) cwla</b>	X.25 call request packet with a host address

Key Word:

U(undo) D(default) Q(quit)

.....

(29)snmp Modify SNMP interface parameters

(30)x25 Set parameters for X.25

Please Input the code of command to be excute(0-30): **30**

.....

(02)cwla Call with/without local address

(03)dbit Use Dbit mode or not

- .....
- (15)nps                      Enable/Disable packet size negotiation
- (16)nui                        Set network user identity
- (17)nws                        Enable/Disable window size negotiation

.....  
 Please Input the code of command to be excute(0-26): **03** ( choose 03,15,17,02 respectively to implement the configuration )

Will you excute it? (Y/N):y

**4.3.7 Configure the X.25-TCP switching parameters**

User can configure the X.25-TCP switching parameters with the following command in interface configuration mode ( this function is not in the formal version but only provided in some probational version)

command	Task
<b>x25 (undo) tcp user-data line</b>	Set the user-data utilized by x25-tcp in the interface
<b>x25 (undo) tcp pkt-format [rfc1006/transparent/user]</b>	Set the switching packet-format
<b>x25 (undo) tcp iso-address line</b>	Set the ISO extension address used by x25-tcp in the interface

Key Word:

Q(quit)

.....

- (29)snmp                      Modify SNMP interface parameters
- (30)x25                        Set parameters for X.25

Please Input the code of command to be excute(0-30): **30**

Key Word:

U(undo)    D(default)                      Q(quit)

.....

- (24)tcp                        Set X25-TCP parameters related
- (25)wsize                      Set X.25 level 3 window size

.....

Please Input the code of command to be excute(0-26): **24**

Key Word:

Q(quit)

- (00)iso-address                      Set X.25 extend ISO address
- (01)pkt-format                      Set X25-TCP switching packet format
- (02)user-data                        Set X.25 user data

.....

Please Input the code of command to be excute(0-5): **0** ( you can input 0、 1、 2 to set various parameters respectively )

Key Word:

Q(quit)

(00)Line                                      Hex ISO address Data

Please Input the code of command to be excute(0-0): **0**

Please input a string:**123456** ( input Hex ISO address Data )

Will you excute it? (Y/N):y

### 4.3.8 configure PVC switching between X.25 interfaces

D-LINK router can be used as X.25 switch. It includes PVC switching and SVC switching. The two interfaces used for PVC switching must has untapped PVC.

In configuration mode, user can use the following commands to set the local PVC switching:

command	task
<b>x25switch (undo) connect</b> port1 port1_pvc_no port2 port2_pvc_no	Set the PVC switching

[DEFAULT@Router /config/]#**x25switch**

Key Word:

U(undo) D(default) Q(quit)

(00)connect Add/delete a PVC route in X.25 switch table

(01)destination Add/delete a SVC route in X.25 switch table

(02)xot Configure X25 over TCP route in X.25 switch table

Please Input the code of command to be excute(0-2): **0**

Key Word:

Q(quit)

(00)Async Async interface

(01)Serial Serial interface

Please Input the code of command to be excute(0-1): **1**

Please input a interface name:**s1/0** (input the interface name)

Key Word:

Q(quit)

(00)<1-15> PVC number

Please Input the code of command to be excute(0-0): **0**

Please input a string:**15**

Key Word:

Q(quit)

(00)Async Async interface

(01)Serial Serial interface

Please Input the code of command to be excute(0-1): **1**

Please input a interface name:**s1/1** (input the interface name)

Key Word:

Q(quit)

(00)<1-15> PVC number

Please Input the code of command to be excute(0-0): **0**

Please input a string:**13**

Will you excute it? (Y/N):**y**

The two connected interface must have valid PVC(permanent virtue circuit) if user want to configure the switching table.

### Configure SVC switching between X.25 interface

The window size and packet length of the host that switch through the D-LINK router can be different, they can be negotiated the minimum value.

Use the following command in configuration mode:

<b>x25switch (undo/default) destination</b> [x121addr/default] port	Set a SVC interface addressing
--	--------------------------------

[DEFAULT@Router /config/]#**x25switch**

Key Word:

U(undo) D(default) Q(quit)

(00)connect Add/delete a PVC route in X.25 switch table  
 (01)destination Add/delete a SVC route in X.25 switch table  
 (02)xot Configure X25 over TCP route in X.25 switch table

Please Input the code of command to be excute(0-2): **1**

Key Word:

Q(quit)

(00)x121addr X.121 address

Please Input the code of command to be exc ute(0-0): **0**

Please input a string:**123456** (input the x121 address)

Key Word:

Q(quit)

(00)Serial Serial interface

Please Input the code of command to be excute(0-0): **0**

Please input a interface name:**s1/0** (input the interface name)

.....

**configuring the XOT switching between X.25 interfaces**

D-LINK router can implement the X.25 datagram switching basing on the TCP/IP.

Use the following command in configuration mode

<b>x25switch (undo) xot pvc</b> <i>local-interface local-pvc remote-interface remote-pvc remote-ip-address [source interface]</i>	Set a PVC XOT interface addressing
<b>x25switch (undo) xot svc</b> <i>x.121-address remote-ip-address [source interface]</i>	Set a SVC XOT interface addressing

1、configuring a PVC XOT interface addressing

[DEFAULT@Router /config/]#**x25switch**

Key Word:

U(undo) D(default) Q(quit)

(00)connect Add/delete a PVC route in X.25 switch table  
 (01)destination Add/delete a SVC route in X.25 switch table  
 (02)xot Configure X25 over TCP route in X.25 switch table

Please Input the code of command to be excute(0-2): **2**

Key Word:

Q(quit)

(00)pvc Add/delete a PVC route based on XOT in X.25 switch table

(01)svc Add/delete a SVC(xot) route in X.25 switch table

Please Input the code of command to be excute(0-1): **0**

Key Word:

Q(quit)

(00)Async async interface

(01)Serial serial interface

Please Input the code of command to be excute(0-1): **1**

Please input a interface name:**s1/0** (input interface name )

Key Word:

Q(quit)  
 (00)<1-15> Local PVC number

Please Input the code of command to be excute(0-0): **0**

Please input a string:**15** ( input pvc number )

Key Word:

Q(quit)  
 (00)Async async interface  
 (01)Serial serial interface

Please Input the code of command to be excute(0-1): **1**

Please input a interface name:**s2/0**

Key Word:

Q(quit)  
 (00)<1-15> Local PVC number

Please Input the code of command to be excute(0-0): **0**

Please input a string:**15**

Key Word:

Q(quit)  
 (00)A.B.C.D remote ip address

Please Input the code of command to be excute(0-0): **0**

Please input a ip address:**10.0.0.1** ( input the remote ip address )

Key Word:

Q(quit)  
 (00)source source interface  
 (01)<cr>

Please Input the code of command to be excute(0-1): **1**

Will you excute it? (Y/N):**y**

## 2、configuring a SVC XOT interface addressing

[DEFAULT@Router /config/]#**x25switch**

Key Word:

U(undo) D(default) Q(quit)

(00)connect Add/delete a PVC route in X.25 switch table

(01)destination Add/delete a SVC route in X.25 switch table

(02)xot Configure X25 over TCP route in X.25 switch table

Please Input the code of command to be excute(0-2): **2**

Key Word:

Q(quit)  
 (00)pvc Add/delete a PVC route based on XOT in X.25 switch table

(01)svc Add/delete a SVC(xot) route in X.25 switch table

Please Input the code of command to be excute(0-1): **1**

Key Word:

Q(quit)  
 (00)WORD Destination X.121 address

Please Input the code of command to be excute(0-0): **0**

Please input a string:**12345678** (input x121 address)

Key Word:

Q(quit)  
 (00)<A.B.C.D> Remote IP Address

Please Input the code of command to be excute(0-0): **0**

Please input a IP Address:**192.168.0.1** ( iput ip address )

Key Word:  
 Q(quit)  
 (00)source local source interface  
 (01)<cr>  
 Please Input the code of command to be excute(0-1):1  
 Will you excute it? (Y/N):y

### Configuring the X.25-TCP switching gateway

D-LINK router can implement the datagram switching between X.25 and TCP/IP.

User the following command in configuration mode:

<b>Translate (undo) tcp ip ip-address svc intr1 x121address1 lport locport rport remport [backup intr2 x121address2]</b>	Set a mapping between the source IP address and destination X.121 address, configure the local and remote TCP monitor interface
<b>translate (undo) tcp ip ip-address pvc intr1 pvc#1 lport locport rport remport [backup intr2 pvc#2]</b>	Set a mapping between the source IP address and destination PVC address, configure the local and remote TCP monitor interface

[DEFAULT@Router /config/]#**translate**

Key Word:  
 U(undo) D(default) Q(quit)  
 (00)x25 Translate to X.25 encapsulation  
 (01)tcp Translate packet between TCP and X.25  
 Please Input the code of command to be excute(0-1): 1  
 Key Word:  
 Q(quit)  
 (00)ip Specified the source IP address  
 Please Input the code of command to be excute(0-0): 0  
 Key Word:  
 Q(quit)  
 (00)<A.B.C.D> Source IP Address  
 Please Input the code of command to be excute(0-0): 0  
 Please input a ip address:10.0.0.1 ( input remote ip address )  
 Key Word:  
 Q(quit)  
 (00)pvc Use pvc to connect to remote  
 (01)svc Use svc to connect to remote  
 Please Input the code of command to be excute(0-1): 1 ( you can also choose 0 to implement the pvc configuration )  
 Key Word:  
 Q(quit)  
 (00)Serial Serial interface  
 Please Input the code of command to be excute(0-0): 0  
 Please input a interface name:s1/0 ( input the interface name )  
 Key Word:  
 Q(quit)  
 (00)WORD Remote X.121 address

Please Input the code of command to be excute(0-0): 0

Please input a string:1234 ( input x121 address )

Key Word:

Q(quit)

(00)lport Specified the local listen port

Please Input the code of command to be excute(0-0): 0

Key Word:

Q(quit)

(00)<1-65535> Listen port number

Please Input the code of command to be excute(0-0): 0

Please input a string:100 ( input Listen port number )

Key Word:

Q(quit)

(00)rport Specified the remote listen port

Please Input the code of command to be excute(0-0): 0

Key Word:

Q(quit)

(00)<1-65535> Listen port number

Please Input the code of command to be excute(0-0): 0

Please input a string:200 ( input Listen port number , remote )

Key Word:

Q(quit)

(00)backup Backup interface configuration

(01)<cr>

Please Input the code of command to be excute(0-1): 1

Will you excute it? (Y/N):y

### Monitoring and maintaining the LAPB and X.25

To monitor and maintain the X.25 and LAPB, use the following commands in configuration mode:

command	Task
<b>clear x25 port vc-number</b>	Clear SVC
<b>show interface serial number</b>	Display the operation statistic of interfaces
<b>show x25</b>	Display the X.25 interface address mapping
<b>show x25switch</b>	Display the X.25 switching table
<b>debug (undo) lapb</b> [iframes sframes uframes raw]serial	Debug the LAPB frames
<b>debug (undo) x25</b> [events normal raw xot]serial	Debug the x25 internal events and datagram
<b>debug x25 (undo) xot</b>	Debug the setup of xot
<b>debug (undo)x25 tcp</b> [data event list]	Debug the events, data receiving and transmitting, link status of x25-tcp

The specifications are given below:

1、 clear SVC

[DEFAULT@Router /enable/#clear

.....

(10)telnet Clear incoming telnet connection

(11)x25 Clear X.25 circuits

Please Input the code of command to be excute(0-11): **11**

(00)Serial                      Serial interface

Please Input the code of command to be excute(0-0): **00**

Please input a interface name:s**0/1** ( input interface name )

(00)<1-16>                      SVC number need to clear

Please Input the code of command to be excute(0-0): **00**

Please input a digital number:Please input a string:**5** ( input the SVC number )

Will you excute it? (Y/N):**y**

## 2、 Display the operation statistic of interfaces

[DEFAULT@Router /enable/]#**show**

.....

(16)hosts                      Host table

(17)interface                      interface status and configuration

.....

Please Input the code of command to be excute(0-45): **17**

(00)FastEthernet                      FastEthernet interface

(01)Serial                      Serial interface

(02)Async                      Asynchronous interface

Please Input the code of command to be excute(0-2):**01**

Please input a interface name:s**0/1** ( input interface name )

Will you excute it? (Y/N):**y**

## 3、 show the address mapping of an X.25 interface

[DEFAULT@Router /config/]#**show**

Key Word:

U(undo)                      D(default)                      Q(quit)

.....

(47)vpdn                                      vpdn group

(48)x25                                      Display X.25 state

.....

Please Input the code of command to be excute(0-50): **48**

Key Word:

Q(quit)

(00)tcp                                      Show X25-TCP State

(01)vc                                      Display X.25 state

(02)xot                                      Show XOT State

Please Input the code of command to be excute(0-2): **1**

Key Word:

Q(quit)

(00)<cr>

Please Input the code of command to be excute(0-0): **0**

Will you excute it? (Y/N):**y**

## 4、 Display the X.25 switching table

[DEFAULT@Router /enable/]#**show**

.....

(43)x25                                      Display X.25 state

(44)x25switch                      Show X.25 switch route table

(45)x29                                      Show X.29d X3 pad parameters

Please Input the code of command to be excute(0-45): **44**

Will you excute it? (Y/N):**y**

## 5、 Debug the LAPB frames

```
[DEFAULT@Router /enable/]#debug
.....
(14)l2tp                L2TP information
(15)lapb                LAPB information
.....
Please Input the code of command to be excute(0-27): 15
(00)iframes            LAPB I frames
(01)raw                LAPB raw frames content
(02)sframes            LAPB S frames
(03)uframes            LAPB U frames
Please Input the code of command to be excute(0-3): 00
(00)interface-name
(01)<cr>
Please Input the code of command to be excute(0-1): 00
Please input a interface name:s0/1 ( input interface name )
Will you excute it? (Y/N):y
```

## 6、 Debug the x25 internal events and datagram

```
[DEFAULT@Router /enable/]#debug
.....
(26)tunnel              Generic Tunnel Interface
(27)x25                 X.25 information
Please Input the code of command to be excute(0-27): 27
(00)events              All non-data packets
(01)normal              All data packets
(02)packet              raw packets
(03)tcp                 Debug X25-TCP
(04)xot                 Debug XOT(X.25-Over-TCP) packet
Please Input the code of command to be excute(0-4): 00
(00)interface-name
(01)<cr>
Please Input the code of command to be excute(0-1): 00
Please input a interface name:s0/1 ( input interface name )
Will you excute it? (Y/N):y
```

## 7、 Debug the setup process of xot

```
[DEFAULT@Router /enable/]#debug
.....
(26)tunnel              Generic Tunnel Interface
(27)x25                 X.25 information
Please Input the code of command to be excute(0-27): 27
(00)events              All non-data packets
(01)normal              All data packets
(02)packet raw packets
(03)tcp                 Debug X25-TCP
(04)xot                 Debug XOT(X.25-Over-TCP) packet
Please Input the code of command to be excute(0-4): 4
(00)<cr>
Please Input the code of command to be excute(0-0): 00
Will you excute it? (Y/N):y
```

## 8. Debug the events, data receiving and transmitting, link status of x25-tcp

```
[DEFAULT@Router /enable/]#debug
.....
(26)tunnel          Generic Tunnel Interface
(27)x25             X.25 information
Please Input the code of command to be excute(0-27): 27
(00)events         All non-data packets
(01)normal         All data packets
(02)packet raw packets
(03)tcp            Debug X25-TCP
(04)xot            Debug XOT(X.25-Over-TCP) packet
Please Input the code of command to be excute(0-4): 3
(00)data           X25TCP data packet
(01)event          X25TCP event
(02)link-status    X25TCP link status
Please Input the code of command to be excute(0-2): 00
Will you excute it? (Y/N):y
```

**X.25 and LAPB configuration examples**

The following sections provide examples to help you understand how to configure LAPB and X.25 for your network:

**Typical LAPB configuration example**

In the following example, the frame size (N1), window size (k), and maximum retransmission (N2) parameters retain their default values. The **encapsulation** interface configuration command sets DCE operation to carry a single protocol, IP by default. The **lapb t1** interface configuration command sets the retransmission timer to 4 seconds for a link with a long delay or slow connecting DTE device.

```
[DEFAULT@Router /enable/]#interface s1/0
[DEFAULT@Router /s1/0/]#encapsulation x25
[DEFAULT@Router /s1/0/]#x25 interface dce
[DEFAULT@Router /s1/0/]#x25 t1 4
```

**Typical X.25 configuration example**

This chapter will introduce some typical X.25 configuration examples to make you understand more about the tasks and contents related with X.25 of D-LINK router. Note that the content after the “!” is not a part of the command but only a remark.

**link two router through the back-to-back serial interface directly**

## ( 1 ) network requirements

User can merely configure these two routers like the figure below if you only need to connect two routers directly through serial interface with the encapsulation of X.25 and IP datagram.

## ( 2 ) Figure

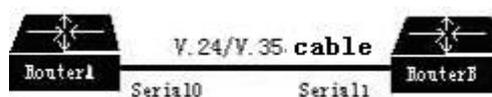


Figure 2 two routers connect directly through a serial interface

## ( 3 ) configuration steps

## configuring router A

## ! Select an interface

```
[DEFAULT@Router /enable/]#cd config
[DEFAULT@Router /config/]#interface s1/0
```

## ! assign an IP address for the interface

```
[DEFAULT@Router /s1/0/]#ip address 202.38.160.1 255.255.255.0
```

```

! set the interface as X.25 interface and set it operates in DTE mode
[DEFAULT@Router /s1/0/]#encapsulation x25
! set the X.121 address of the interface
[DEFAULT@Router /s1/0/]#x25 address 20112451
! specify the address mapping to the peer end in the network
[DEFAULT@Router /s1/0/]#x25 map 202.38.160.2 svc 20112452
! configuring router B
! select an interface
[DEFAULT@Router /enable/]#cd config
[DEFAULT@Router /config/]#interface s1/0
! assign an IP address for the interface
[DEFAULT@Router /s1/0/]#ip address 202.38.160.2 255.255.255.0
! set the interface speed
[DEFAULT@Router /s1/0/]#physical-layer speed 64000
! set the interface as X.25 interface and set it operates in DCE mode
[DEFAULT@Router /s1/0/]#encapsulation x25
[DEFAULT@Router /s1/0/]#x25 interface dce
! set the X.121 address of the interface
[DEFAULT@Router /s1/0/]#x25 address 20112452
! specify the address mapping to the peer end of the network
[DEFAULT@Router /s1/0/]#x25 map 202.38.160.1 svc 20112451

```

### Connecting the router to X.25 public packet network

#### ( 1 ) network requirement

Router A,B,C are connected to the same X.25 network to communicate with each other, as the following figure, the configurations are:

The IP address of these routers are 168.173.24.1, 168.173.24.2 and 168.173.24.3 ;

Routers X.121 address assigned by the network are 30561001, 30561002, 30561003

The standard receiving and transmitting window size supported by the packet network are both 5.

The standard maximum receiving and transmitting packet length are both 512

#### ( 2 ) Figure

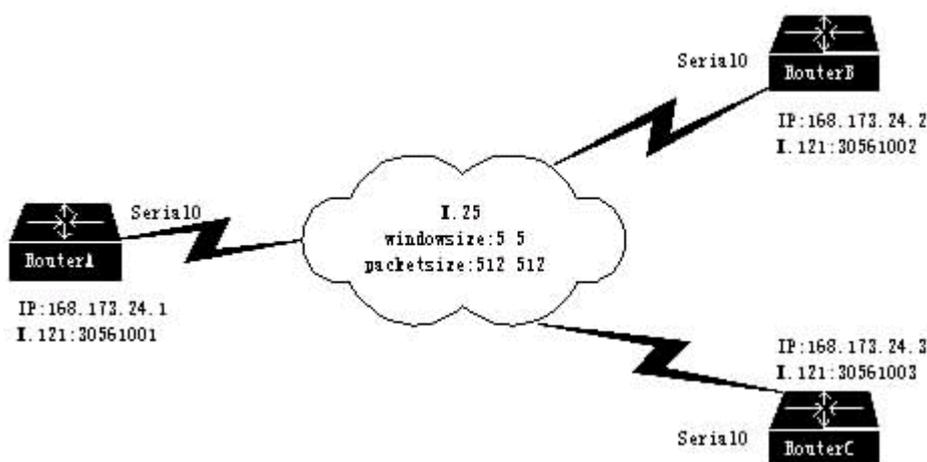


Figure 3 connect the router to X.25 community packet network

#### ( 3 ) configuration steps

configuring Router A

! Configuring the interface IP address

```

[DEFAULT@Router /enable/]#cd config
[DEFAULT@Router /config/]#interface s1/0
[DEFAULT@Router /s1/0/]#ip address 168.173.24.1 255.255.255.0

```

! Connect to public packet network and make the router operate as DTE:

```
[DEFAULT@Router /s1/0/]#encapsulation x25
[DEFAULT@Router /s1/0/]#x25 address 30561001
[DEFAULT@Router /s1/0/]#x25 htc 32
[DEFAULT@Router /s1/0/]#x25 map 168.173.24.2 svc 30561002
[DEFAULT@Router /s1/0/]#x25 map 168.173.24.3 svc 30561003
```

Configuring Router B

! Configuring the interface IP address

```
[DEFAULT@Router /enable/]#cd config
[DEFAULT@Router /config/]#interface s1/0
[DEFAULT@Router /s1/0/]#ip address 168.173.24.2 255.255.255.0
```

! Connect to public packet network and make the router operate as DTE:

```
[DEFAULT@Router /s1/0/]#encapsulation x25
[DEFAULT@Router /s1/0/]#x25 address 30561002
[DEFAULT@Router /s1/0/]#x25 htc 32
[DEFAULT@Router /s1/0/]#x25 map 168.173.24.1 svc 30561001
[DEFAULT@Router /s1/0/]#x25 map 168.173.24.3 svc 30561003
```

Configuring Router C

!Configuring the interface IP address

```
[DEFAULT@Router /enable/]#cd config
[DEFAULT@Router /config/]#interface s1/0
[DEFAULT@Router /s1/0/]#ip address 168.173.24.3 255.255.255.0
```

! connect to public packet network and make the router operate as DTE:

```
[DEFAULT@Router /s1/0/]#encapsulation x25
[DEFAULT@Router /s1/0/]#x25 address 30561003
[DEFAULT@Router /s1/0/]#x25 htc 32
[DEFAULT@Router /s1/0/]#x25 map 168.173.24.1 svc 30561001
[DEFAULT@Router /s1/0/]#x25 map 168.173.24.2 svc 30561002
```

### 4.3.9 Configuring the virtue circuit ranges

Perform the following commands to set the router's interface serial 1/0 to be encapsulated with X.25, and the ranges of virtue circuit are: PVC [1,8] ,SVC [9,64].

```
[DEFAULT@Router /enable/]#cd config
[DEFAULT@Router /config/]#interface s1/0
[DEFAULT@Router /s1/0/]#encapsulation x25
[DEFAULT@Router /s1/0/]#x25 htc 64
[DEFAULT@Router /s1/0/]#x25 pvc 8
```

Configuration example of XOT based on PVC

The configuration commands and arrangement plan are as follows:

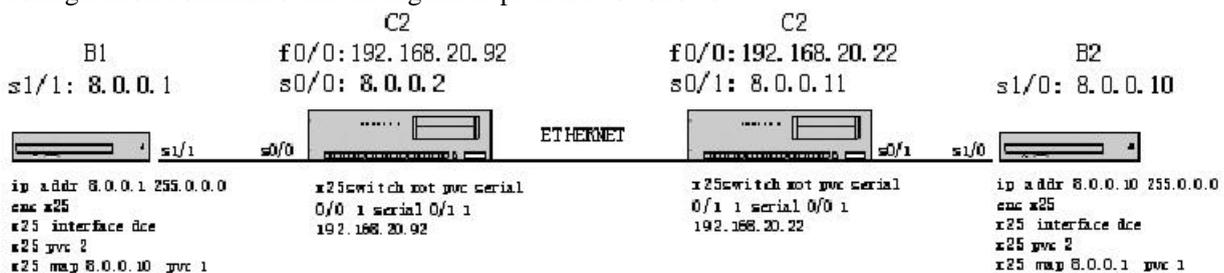


Figure 4 arrangement plan of XOT based on PVC

Configuring router B1:

```
[DEFAULT@Router /s1/1/]#ip address 8.0.0.1 255.0.0.0
```

```
[DEFAULT@Router /s1/1/#enc x25
[DEFAULT@Router /s1/1/#x25 interface dce
[DEFAULT@Router /s1/1/#x25 pvc 2
[DEFAULT@Router /s1/1/#x25 map 8.0.0.10 pvc 1
Configure router C1:
[DEFAULT@Router /f0/0/#ip address 192.168.20.92 255.0.0.0
[DEFAULT@Router /s1/0/#ip address 8.0.0.2 255.0.0.0
[DEFAULT@Router /s1/0/#enc x25
[DEFAULT@Router /s1/0/#x25 pvc 2
[DEFAULT@Router /config/#x25switch xot pvc serial 1/0 1 serial 1/1 1 192.168.20.22
```

### Configuring router C2

```
[DEFAULT@Router /f0/0/#ip address 192.168.20.22 255.0.0.0
[DEFAULT@Router /s1/1/#ip address 8.0.0.11 255.0.0.0
[DEFAULT@Router /s1/1/#enc x25
[DEFAULT@Router /s1/1/#x25 pvc 2
[DEFAULT@Router /config/#x25switch xot pvc serial 1/1 1 serial 1/0 1 192.168.20.92
```

### Configuring router B2:

```
[DEFAULT@Router /s1/0/#ip address 8.0.0.10 255.0.0.0
[DEFAULT@Router /s1/0/#enc x25
[DEFAULT@Router /s1/0/#x25 interface dce
[DEFAULT@Router /s1/0/#x25 pvc 2
[DEFAULT@Router /s1/0/#x25 map 8.0.0.1 pvc 1
```

## Configuring X.25-TCP switching examples

The configuration commands and arrangement plan are as follows:

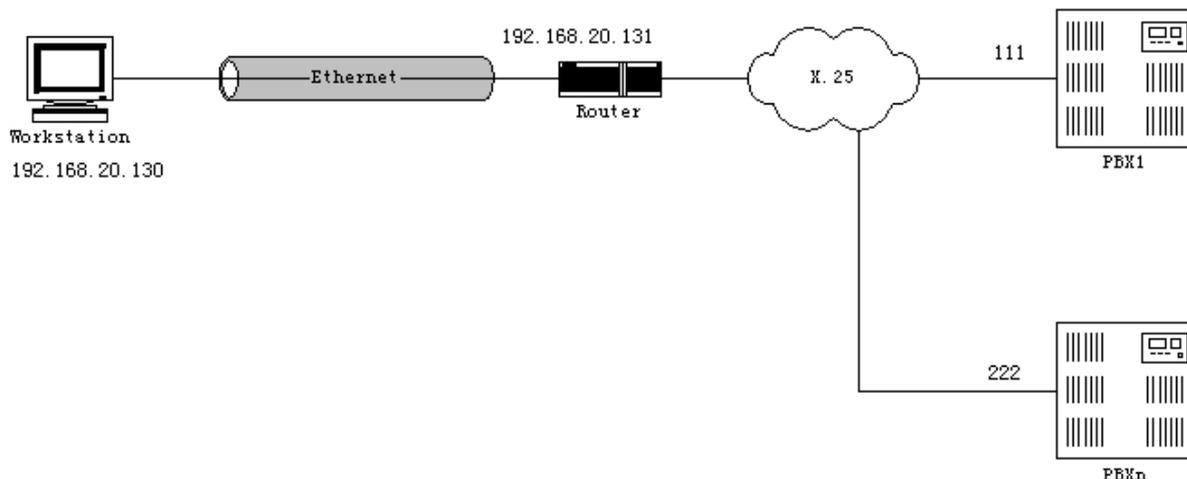


Figure 5 arrangement plan of X25-TCP

### Configuring router B1:

```
[DEFAULT@Router /config/#translate tcp ip 192.168.20.130 svc s1/0 111 lport 2000 rport 2000
[DEFAULT@Router /s1/0/# encapsulation x25
[DEFAULT@Router /s1/0/# x25 address 222
[DEFAULT@Router /s1/0/# x25 tcp user-data 03010100
[DEFAULT@Router /s1/0/# x25 tcp pkt-format RFC1006
[DEFAULT@Router /s1/0/# x25 tcp iso-address 000fc909103600001111cb09103600002222
[DEFAULT@Router /s1/0/# ip address 192.168.20.131 255.255.255.
```

## 4.4 Configuring X.25 PAD Operation Task List

### 4.4.1 Network Topology

This chapter describes how to make connections with remote devices using the X.25 protocol by PAD operation.

For a complete description of the PAD commands in this chapter, refer to the *WANs Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

### 4.4.2 About Network Topology

PADs are configured to enable X.25 connections between network devices. A PAD is a device that receives a character stream from one or more terminals, assembles the character stream into packets, and sends the data packets out to a host. A PAD can also do the reverse. It can take data packets from a network host and translate them into a character stream that can be understood by the terminals. A PAD is defined by CCITT Recommendations X.3, X.28, and X.29.

Figure 1 shows a remote X.25 user placing a call through an X.25 switched network, to the internal PAD application on a D-Link router, and to an X.25 host located inside a corporate data center.

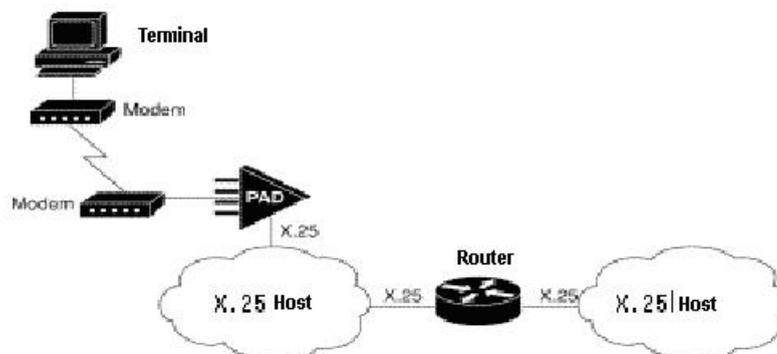


Figure 1 Standard X.25 Connection Between a Dumb Terminal and an X.25 Host

PADs can also be configured to work with a protocol translation application. Figure 87 shows an example of a remote PC placing an analog modem call to an IP network, connecting to a D-LINK 4500-M router, allowing its IP packets to undergo an IP-to-X.25 protocol translation, which in turn communicates with an internal PAD device and establishes a connection with an X.25 host.

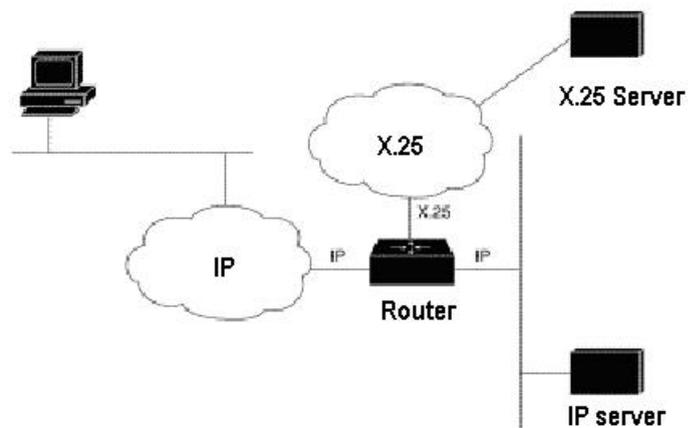


Figure 2: PC Dialing In to an X.25 Host Using Protocol Translation

### Use PAD Mode

The following sections describe how to use the PAD standard user interface to make X.25 PAD connections:

? [Description](#)

- ? [Application](#)
- ? [Configuration Task List](#)
- ? [Example](#)

### Description

X.28 emulation is the standard user interface between data terminal equipment (DTE) and a packet assembler/disassembler (PAD). The D-Link router provides an X.28 user emulation mode, which enables you to interact with and control the PAD. During this exchange of control information, messages or commands sent from the terminal to the PAD are called PAD command signals. Messages sent from the PAD to the terminal are called PAD service signals. These signals and any transmitted data take the form of encoded character streams as defined by International Alphabet Number 5.

For asynchronous devices such as terminals or modems to access an X.25 network host, the device's packets must be assembled or disassembled by a PAD device. Using standard X.28 commands from the PAD, calls can be made into an X.25 network, X.3 PAD parameters can be set, or calls can be reset. X.3 is the ITU-T recommendation that defines various PAD parameters used in X.25 networks. There are 22 available X3 PAD parameters to configure. X.3 PAD parameters are internal variables that define the operation of a PAD. For example, parameter number 9 is the crpad parameter. It determines the number of bytes to add after a carriage return. X.3 parameters can also be set by a remote X.25 host using X.29. (See Figure 3.)

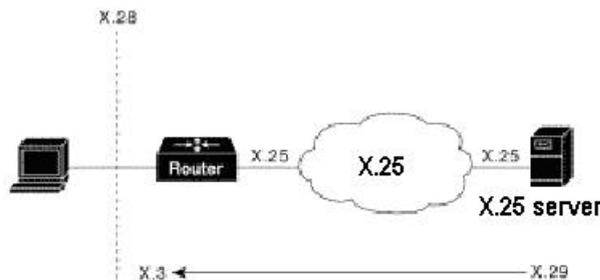


Figure 3 Asynchronous Device Dialing In to an X.25 Host over an X.25 Network

### Application

X.28 enables PAD system administrators to dial into X.25 networks or set PAD parameters using the X.28 standard user interface. This standard interface is commonly used in many European countries. It adheres to the X.25 International Telecommunication Union Telecommunication (ITU-T) standards.

The X.28 interface is designed for asynchronous devices that require X.25 transport to access a remote or native asynchronous or synchronous host application. For example, dial-up applications can use the X.28 interface to access a remote X.25 host. X.28 PAD calls are often used by banks to support back office applications such as ATM machines, point of sales authorization devices, and alarm systems. An ATM machine may have an asynchronous connection to an alarm host and a D-Link router. When the alarm is tripped, the alarm sends a distress call to the authorities via the D-Link router and a X.28 PAD call.

D-Link router's X.28 PAD calls can be transported over a public packet network, a private X.25 network, the Internet, a private IP-based network, or a Frame Relay network. X.28 PAD can also be used with protocol translation. Protocol translation and VTY asynchronous interfaces enable users to bidirectionally access an X.25 application with the PAD service or other protocols such as Digital Equipment Corporation (DEC), local-area transport (LAT), and transmission control protocol (TCP).

#### 4.4.3 Configuration Task List

The following optional tasks are described in this section:

- ? [Place and Clear Calls](#)

? [Customize X.3 Parameters](#)

? [Monitor X.25 PAD Connection](#)

Access X.28 mode using the x28 EXEC command *pad*. Then push the Ctrl-p to enter pad mode. the default PAD mode prompt is character “pad” and the symbol “>“. After complete pad>, you can use the standard PAD user interface and configure PAD.

#### 4.4.4 Place and Clear Calls

Many X.25-related functions can be performed in PAD mode, such as placing and clearing calls. Table 20 lists the available PAD command signals that can be issued.

In X.28 mode, there are various PAD command signals you can use. You can choose to use the standard or extended command syntax. For example, you can enter the **clr** command or **clear** command to clear a call. A command specified with standard command syntax is merely an abbreviated version of the extended syntax version. Both syntaxes function the same.

Command	Purpose
Clr	Clear a virtual call.
Help	Display help information.
Int	Send an interrupt packet.
par? Par	Show the current values of local parameters.
Prof filename	Load a standard profile.
Reset	Reset the call.
Set	Change the local values of parameters.
set?	Changes and then read the values of parameters.
Stat	Requests status of a connection.
Quit	Exit PAD connection.

#### 4.4.5 Place a Call

you need to designate the X.121 address of information destination to setup a call with it. Perform the following commands in user mode or management mode:

<b>pad svc</b> <i>address</i> [ <i>profile-number</i> [ <i>r w</i> ]]	Call a remote interface through SVC. If succeed, then enter the X.28 mode and display the “>” prompt.
<b>pad pvc</b> <i>interface pvc#</i> [ <i>profile-number</i> [ <i>r w</i> ]]	Call a remote interface through PVC. If connected, then enter the X.28 mode and display the “>” Prompt.

1、SVC section :

[DEFAULT@Router /enable/]#**pad**

Key Word:

U(undo) D(default) Q(quit)

(00)svc pad to the remote x121 address

(01)pvc pad to the remote through pvc

Please Input the code of command to be excute(0-1): **1** ( you can also input 0 to set pvc )

Key Word:

Q(quit)

```
(00)WORD X.121 address
Please Input the code of command to be excute(0-0): 0
Please input a string:1234 (input the x121 address)
Key Word:
Q(quit)
(00)<0-31> X29 pad profile number
(01)<cr>
Please Input the code of command to be excute(0-1): 0
Please input a string: 5 ( input profile number )
Key Word:
Q(quit)
(00)r X29 pad profile read-only
(01)w X29 pad profile read-write
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00<cr>
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y
```

#### 4.4.6 Clear a Call

After you connect to a remote X.25 device, you can clear the connection by using the following commands :

Step	Command	Purpose
1	ctrl-p	From the remote host, escape back to the local router PAD mode.
2	Clr	Clear the virtual call.

#### 4.4.7 Customerize Local X.3 Parameter

To set an X.3 PAD parameter from a local terminal, use the following commands beginning in EXEC mode or User mode:

Step	Command	Purpose
1	<b>pad</b> <i>address</i>	Enter X.28 mode.
3	Ctrl-p	From X.28 mode escape back to PAD mode.
4	<b>par</b>	Display the current X.3 PAD parameters.
5	<b>set</b> <i>parameter-number: new-value</i>	Change the value of a parameter.
6	<b>par</b>	Verify that the new PAD parameter was set correctly.

[DEFAULT@Router /enable/]#**pad**

```
Key Word:
U(undo) D(default) Q(quit)
(00)svc pad to the remote x121 address
(01)pvc pad to the remote through pvc
Please Input the code of command to be excute(0-1): 1 ( you could also input 0 to configure the pvc )
Key Word:
```

Q(quit)  
 (00)WORD X.121 address  
 Please Input the code of command to be excute(0-0): **0**  
 Please input a string:**1234** (input the x121 address)  
 Key Word:  
 Q(quit)  
 (00)<0-31> X29 pad profile number  
 (01)<cr>  
 Please Input the code of command to be excute(0-1): **1**  
 Will you excute it? (Y/N):**y**

#### 4.4.8 Monitor X.25 PAD Connection

To display currently opened connecting information, use the following EXE mode command:

Command	Purpose
Show x25	To display currently opened X.25 connecting information

```
[DEFAULT@Router /config/]#show
Key Word:
.....
(47)x25 Display X.25 state
(48)x25switch Show X.25 switch route table
(49)x29 Show X.29d X3 pad parameters
Please Input the code of command to be excute(0-49): 47
Key Word:
Q(quit)
(00)tcp Show X25-TCP State
(01)vc Display X.25 state
(02)xot Show XOT State
Please Input the code of command to be excute(0-2): 1
Key Word:
Q(quit)
(00)<cr>
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y
```

This information includes current status of virtual circuit.

#### 4.4.8 X.25 PAD access limitation

This configuration can limit the source X121 address accessing the router.

Command	function
<b>X25 map pad x121addr</b>	Configuring the source X121 address for the static useful pad to access the router
<b>X25 pad-access</b>	Enable the pad-access limitation, the configuration will be checked by using the item configured by the upper command. If it has not been configured, all the pad access will be forbidden.

Input the following commands in the interface configurative mode:

```
[DEFAULT@Router /s0/1/]#x25
.....
(11)map Set map from IP address to X.121 address
```

```
(12)mod          Set LAPB and X.25 module(8/128)
.....
Please Input the code of command to be excute(0-26): 11
(00)A.B.C.D      IP address
(01)pad          pad links
Please Input the code of command to be excute(0-1): 01
(00)WORD         originating X121 address
Please Input the code of command to be excute(0-0): 00
Please input a string:123456 ( input the x121 address , here is just a example )
Will you excute it? (Y/N):y
    [DEFAULT@Router /s0/1/]#x25
.....
(25)wsize        Set X.25 level 3 window size
(26)pad-access   Accept only PAD connections from statically mapped X25 hosts
Please Input the code of command to be excute(0-26): 26
Will you excute it? (Y/N):y
```

#### 4.4.9 PAD Signal Examples

The following examples show two ways to make a call to a remote X.25 host over a serial line. The remote host's interface address is 123456. Router-A calls router-B using the **pad 123456 EXEC** command.

```
[DEFAULT@RouterA /enable/]#pad svc 123456
COM
[DEFAULT@RouterB /]# exit
CLR(cause=0x0,diag=0x0)
[DEFAULT@RouterA /enable/]#
```

The following examples is to clear a connection with a remote X.25 host. Router-A disconnecting from router-B using the X.28 mode **clr** command.

```
[DEFAULT@RouterA /enable/]#pad svc 123456
COM
[DEFAULT@RouterB /]# Ctrl-p
pad>clr
CLR CONF
Pad>
```

#### 4.4.10 X.3 Customization Examples

The following example configures parameter 9 from 0 to 1, which adds one byte after the carriage return. This setting is performed from a local terminal using the **set parameter-number: new-value PAD** command signal.

```
[DEFAULT@RouterA /enable/]# pad svc 12345678
[DEFAULT@RouterB /]# ctrl-p
pad>par
PAR 1:1 2:1 3:126 4:0 5:1 6:2 7:2 8:0 9:0 10:0 11:14 12:1 13:0 14:0 15:0 16:127 17:24 18:18 19:2 20:0
21:0 22:0
pad> set 9:1
pad> par
PAR 1:1 2:1 3:126 4:0 5:1 6:2 7:2 8:0 9:1 10:0 11:14 12:1 13:0 14:0 15:0 16:127 17:24 18:18 19:2 20:0
21:0 22:0
pad>
```

#### 4.4.11 X.3 Profile Example

The following example modifies and loads an existing X.25 PAD parameter profile. It accesses the existing PAD profile *ppp*, changes its padding parameter (specified as 9) to a value of 2, and displays the new parameters using the **par** command in PAD mode.

```
[DEFAULT@RouterA /enable/]# pad 3333
[DEFAULT@RouterB /]# ctrl-p
pad>prof 0
pad>par
PAR 1:1 2:1 3:126 4:0 5:1 6:2 7:2 8:0 9:2 10:0 11:14 12:1 13:0 14:0 15:0 16:127 17:24 18:18 19:2 20:0
21:0 22:0
```

Note: If the X.29 profile is set to default, the profile is applied to all incoming X.25 PAD calls, including the calls used for protocol translation.

#### 4.4.12 Getting Help Example

Use the help command to get short descriptions of the available parameters.

```
pad> help
CLR - clear X.25 connection
HELP - this help
INT - send interrupt packet over X.25 connection
PAR? - show X.3 parameters as wanted
PROF - use X.3 profile 0 or 1
QUIT - quit PAD and clear connection
RESET - send RESET packet over X.25 connection
SET - set X.3 parameters
SET? - set X.3 parameters and show it
STAT - show X.25 connection status
```

#### 4.4.13 Monitoring X.25 Network Example

Following is show x25 command output example:

```
[DEFAULT@RouterA /enable/]# pad svc 123456789
COM
[DEFAULT@RouterB /]# ent
[DEFAULT@RouterB /enable/]#show x25
X.25/IP state
Serial1/0=UP
=====
No.Port      VC   I/O   State   X.121addr   IPAddr      hostname
=====
01 Serial1/0 16   in    work    1111
[DEFAULT@RouterB /enable/]#
```

### 4.5 Configuring PPP Task List

This section describes how to configure the Point-to-Point Protocol(PPP).(PPP).This section also describe the address pool responding point-to-point connection that apply to asynchronous serial, synchronous serial and ISDN interface.

For complete description of PPP command, refer to “PPP Command Reference” chapter.

### 4.5.1 Implementation Information

PPP, described in RFC 1661, encapsulates network layer protocol information over point-to-point links. You can configure PPP on the following types of physical interfaces:

- Asynchronous serial
- ISDN
- Synchronous serial

By enabling PPP encapsulation on physical interfaces, PPP can also be in effect on calls placed by the dialer interfaces that use the physical interfaces.

The current D-Link router software implementation of PPP supports coordinating option 2: asynchronous control character image; option 3: authentication using CHAP or PAP; option 5, Magic Number configuration options; option 7: compression of protocol domain; option 8: compression of address and control domain. During LCP coordination, the software always sends negotiating options 5, 7 and 8. The negotiating option 2 will be send if it is in the asynchronous mode. If authentication configured, the software sends negotiating option 3.

The software supports LCP negotiating option 5(magic number) on all the serial interfaces. PPP always negotiates magic number to examing loopback on circuit.

D-Link router software supports CHAP and PAP authentication protocol in PPP. For detailed information of authentication, refer to “[Security Configuration Guide](#)”.

### 4.5.2 PPP Configuration Task List

To configure PPP on a serial interface (including ISDN), perform the following required task in interface configuration mode:

#### Enabling PPP Encapsulation

You can also complete the tasks in the following sections; these tasks are optional but offer a variety of uses and enhancements for PPP:

#### Enabling CHAP or PAP Authentication

#### Start Call Back Control Protocol(CBCP)

#### Configuring IP Address Pooling

#### Disabling or Reenabling Peer Host Routes

#### Configuring Multilink PPP

Please see the “[PPP Configuration Example](#)“ chapter.

### 4.5.3 Enabling PPP Encapsulation

To enable PPP on serial lines to encapsulate IP and other network protocol datagrams, use the following command in interface configuration mode:

Command	Purpose
<b>encapsulation ppp</b>	Enabling PPP encapsulation

Key Word:

U(undo) D(default) Q(quit)

.....

(1)encapsulation Set encapsulation type for an interface

(12)english help message in English

.....

Please Input the code of command to be excute(0-32): **11**

Key Word:  
U(undo) D(default) Q(quit)  
(00)frame-relay Frame Relay Protocol  
(01)hdlc HDLC Protocol  
(02)ppp PPP Protocol  
(03)sdlc SDLC Protocol  
(04)x25 X.25 Protocol  
Please Input the code of command to be excute(0-4): 2  
Will you excute it? (Y/N):y

#### 4.5.4 Enabling CHAP or PAP Authentication

PPP with CHAP or PAP authentication is often used to inform the central site about which remote routers are connected to it.

CHAP and PAP were originally specified in RFC 1334, and CHAP is updated in RFC 1994. These protocols are supported on synchronous and asynchronous serial interfaces. When using CHAP or PAP authentication, each router or access server identifies itself by a name. This identification process prevents a router from placing another call to a router to which it is already connected, and also prevents unauthorized access.

Access control using CHAP or PAP is available on all serial interfaces that use PPP encapsulation. The authentication feature reduces the risk of security violations on your router or access server.

**Note: To use CHAP or PAP, you must be running PPP encapsulation.**

When CHAP is enabled on an interface and a remote device attempts to connect to it, the local router or access server sends a CHAP packet to the remote device. The CHAP packet requests or "challenges" the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router.

The required response has two parts:

- ? An encrypted string of the ID, a secret password, and the random number
- Either the host name of the remote device or the name of the user on the remote device

When the local router or access server receives the response, it verifies the secret password by performing the same encryption operation as indicated in the response and looking up the required host name or username. The secret passwords must be identical on the remote device and the local router.

Because this response is sent, the password is never sent in clear text, preventing other devices from stealing it and gaining illegal access to the system. Without the proper response, the remote device cannot connect to the local router.

CHAP transactions occur only when a link is established. The local router or access server does not request a password during the rest of the call. (The local device can, however, respond to such requests from other devices during a call.)

When PAP is enabled, the remote router attempting to connect to the local router or access server is required to send an authentication request. If the username and password specified in the authentication request are accepted, the D-Link router sends an authentication acknowledgment.

After you have enabled CHAP or PAP, the local router or access server requires authentication from remote devices. If the remote device does not support the enabled protocol, no traffic will be passed to that device.

To use CHAP or PAP, you must perform the following tasks:

1. Enable PPP encapsulation.
2. Enable CHAP or PAP on the interface.
3. For CHAP, configure host name authentication and the secret or password for each remote system with which authentication is required.

To enable PPP encapsulation, use the following command in interface configuration mode:

Command	Purpose
<b>encapsulation ppp</b>	Enables PPP encapsulation on an interface.

To enable CHAP or PAP authentication on an interface configured for PPP encapsulation, use the following command in interface configuration mode:

Command	Purpose
<b>ppp authentication { chap   ms-chap   pap } [ word   default ] [ callin ]</b>	Defines the authentication methods supported and the order in which they are used.

Key Word:

Q(quit)

.....

(26)ppp

Point-to-point protocol

(27)priority-group

Assign a priority group to interface

.....

Please Input the code of command to be excute(0-34): **26**

Key Word:

U(undo) D(default)

Q(quit)

(00)authentication

Set PPP link authentication method

(01)authorization

Set PPP network authorization method

.....

Please Input the code of command to be excute(0-9): **0**

Key Word:

Q(quit)

(00)chap

Challenge Handshake Authentication Protocol (CHAP)

(01)ms-chap

Microsoft Challenge Handshake Authentication

Protocol(MS-CHAP)

(02)pap

Password Authentication Protocol (PAP)

Please Input the code of command to be excute(0-2): **0**

Key Word:

Q(quit)

(00)WORD

Use an authentication list with this name

(01)callin

Authenticate remote on incoming call only

.....

Please Input the code of command to be excute(0-5): **0**

Please input a string:**bdcom** ( input authentication list name )

Will you excute it? (Y/N):**y**

To specify the password to be used in CHAP or PAP caller identification, use the following command in global configuration mode:

Command	Purpose
<b>username</b> <i>name</i> <b>password</b> <i>secret</i>	Configures identification.

[DEFAULT@Router /config/]#**username**

Key Word:

U(undo) D(default) Q(quit)

(00)WORD User name

Please Input the code of command to be excute(0-0): **0**

Please input a string:**bdcom** ( input username )

Key Word:

Q(quit)

.....

(05)password Specify the password for the user

(06)trust-host Set user trust host

Please Input the code of command to be excute(0-8): **5**

Key Word:

Q(quit)

(00)0 Specifies an UNENCRYPTED password will follow

(01)7 Specifies a HIDDEN password will follow

(02)LINE The UNENCRYPTED <cleartext> user password

Please Input the code of command to be excute(0-2): **0**

Key Word:

Q(quit)

(00)LINE The UNENCRYPTED <cleartext> user password

Please Input the code of command to be excute(0-0): **0**

Please input a string:**1234567** ( input password )

Key Word:

Q(quit)

.....

(06)user-maxlinks Limit the user's number of inbound links

(07)<cr>

Please Input the code of command to be excute(0-7): **7**

Will you excute it? (Y/N):**y**

Make sure this password does not include spaces or underscores.

#### 4.5.5 Start Callback Control Protocol(CBCP)

In CBCP, the side that launching the dial is Caller, the side that receiving the dial is Answerer.

During the LCP negotiation, if both sides agree to apply the CBCP, thus the CBCP will be run after the authentication period.

During the Callback period, Answerer sends Callback Request and list the Callback options that can be received by Caller.

While Caller responsing by Callback Response, the request options will be listed.

If Callback Response that returns from Caller is legality and can be received by Answerer, then Answerer will respons by Callback Ack. Caller will enter the period of Link Termination and prepare to receive the call after received Callback Ack.

If you need to use CBCP, Caller need to be configured with **config-ppp callback request cbcp**(if the telephone number is specified by caller, you should configure **set-dialer caller xx**).

Except configure **config-ppp callback accept**, if the need no callback, the telephone number of callback need not to be configured by Answerer; if the telephone number is specified by Caller, **user xx password xx callback-dialstring \*** or **set-dialer called\*** should be configured; if the telephone number is specified by Answerer, **user xx password xx callback-dialstring xx** should be configured; if Caller need to select a number form a group of numbers that provided by

Answerer, **set-dialer called xx ; xx ; xx** should be configured.

To use CBCP protocol, you must perform the following tasks:

**Step 1:** Enable PPP Encapsulation

Command	Purpose
<b>encapsulation ppp</b>	Enable PPP on interface.

**Step 2:** configure CBCP on this interface

Command	Purpose
<b>ppp callback request cbcp</b>	Configure to start CBCP negotiation on Caller.
<b>ppp callback accept</b>	Configure to start the receiving of CBCP negotiation on Answerer.

Key Word:

Q(quit)

.....

(26)ppp

Point-to-point protocol

(27)priority-group

Assign a priority group to interface

.....

Please Input the code of command to be excute(0-34): **26**

Key Word:

U(undo) D(default)

Q(quit)

(00)authentication

Set PPP link authentication method

(01)authorization

Set PPP network authorization method

(02)callback

Set CALLBACK parameters

.....

Please Input the code of command to be excute(0-9): **2**

Key Word:

Q(quit)

(00)accept

Accept a callback request

(01)initiate

Initiate callback without PPP callback

negotiation

(02)request

Request a callback

Please Input the code of command to be excute(0-2): **2**

Key Word:

Q(quit)

(00)authentication

Request a callback of authentication

(01)cbcp

Request a callback of cbcp

(02)<cr>

Please Input the code of command to be excute(0-2): **1**

Will you excute it? (Y/N):y

**Step 3:** configure callback telephone number

Command	Purpose
<b>dialer caller xx</b>	Configure the callback telephone number that specified by Caller.

```
user xx password xx callback-dialstring { * | xx }
dialer called { * | xx ; xx ; xx }
```

Configure the telephone number on Answerer that the number is specified by Caller, or specified by Answerer, or select one from Answerer provided numbers by Caller.

1、 configuring the callback dialstring designated by Caller on the caller/called:

[Key Word:

Q(quit)

.....

(09)description

Set the interface description

(10)dialer

Dial-on-demand routing (DDR) commands

.....

Please Input the code of command to be excute(0-32): **10**

Key Word:

U(undo)

D(default)

Q(quit)

(00)called

Dialer called string

(01)caller

Dialer caller string

.....

Please Input the code of command to be excute(0-11): **1** ( you could also choose 0 to configure the called dialstring )

Key Word:

Q(quit)

(00)WORD

Specify calling telephone number to be screened

Please Input the code of command to be excute(0-0): **0**

Please input a string:**12345678** ( input caller dialstring )

Will you excute it? (Y/N):**y**

2、 configuring the dialstring designated by Caller on the Answerer.

Input "user" in the configurative mode, it will prompt:

```
[DEFAULT@Router /config/]#user
```

Key Word:

U(undo)

D(default)

Q(quit)

(00)WORD

User name

Please Input the code of command to be excute(0-0): **0**

Please input a string:**bdcom** ( input username )

Key Word:

Q(quit)

(00)autocommand

Automatically issue a command after the user logs in

(01)callback-dialstring

Callback dialstring

.....

Please Input the code of command to be excute(0-8): **1**

Key Word:

Q(quit)

(00)dial-string

Dialstring

Please Input the code of command to be excute(0-0): **0**

Please input a string:**123456** ( input password )

Key Word:

Q(quit)

.....

(06)user-maxlinks

Limit the user's number of inbound links

(07)<cr>

```
Please Input the code of command to be excute(0-7): 7
Will you excute it? (Y/N):y
```

Answerer has the priority to inquire **user xx password xx callback-dial string**, and then inquire **set-dialer called xx**. In addition, use the symbol “,” to separate the central telephone number and branch number, use the symbol “;” to separate the different numbers. The symbol “\*” indicates the telephone number that specified by Caller.

#### 4.5.6 Configuring IP Address Pool

A point-to-point interface must be able to provide a remote node with its IP address through the IP Control Protocol (IPCP) address negotiation process. The IP address can be obtained from a variety of sources. The address can be configured through the command line, entered with an EXEC-level command, provided by TACACS+ or from a locally administered pool.

#### 4.5.7 Peer Address Allocation

A peer IP address can be allocated to an interface through several methods:

- **IPCP negotiation**—If the peer presents a peer IP address during IPCP address negotiation and no other peer address is assigned, the presented address is acknowledged and used only in the current session.
- **Default IP address**—The peer default ip address can be used to define by **config-peer default ip address** command.
- **TACACS+ assigned IP address or IP address pooling**—During the authorization phase of IPCP address negotiation, TACACS+ can return an IP address that the user being authenticated on a dialup interface can use.
- **Local address pool**—The local address pool contains a set of contiguous IP addresses (a maximum of 1024 addresses) stored in two queues. The free queue contains addresses are stored to the free queue in first-in, first-out (FIFO) order to minimize the chance the address will be reused, and to allow a peer to reconnect using the same address that it used in the last connection. If the address is available, it is assigned; if not, another address from the free queue is assigned.

#### 4.5.8 Precedence Rules

The following precedence rules of peer IP address support determine which address is used. Precedence is listed from most likely to least likely:

1. An address from a local IP address pool or DHCP (typically not allocated unless no other address exists)
2. Configured address from the **peer default ip address** command or address from the **protocol translate** command
3. AAA/TACACS+ provided address or addresses from the pool named by AAA/TACACS+
4. Peer provided address from IPCP negotiation (not accepted unless no other address exists)

#### 4.5.9 Interfaces Affected

Address pooling is available on all asynchronous serial, synchronous serial, ISDN BRI, and ISDN PRI interfaces running PPP.

#### 4.5.10 Configuring IP Address Assignment for each Interface

1. Define an IP address pool for a specific interface.
2. Specify one IP address to be assigned to all dial-in peers on an interface.

To define an IP address pool for use on an interface, use the following commands:

Command	Purpose
<b>ip local pool</b> <i>poolname</i> { <i>begin-ip-address</i> [ <i>ip-address-number</i> ]}	Creates one or more local IP address pools.

<b>interface</b> <i>type number</i>	Specifies the interface and enters interface configuration mode.
<b>peer default config-ip addrpool</b> <i>pool-name</i>	Specifies the address pool for the interface to use.

Please refer to the following example for the order of these commands:

[DEFAULT@Router /config/#**ip**

Key Word:

U(undo) D(default) Q(quit)

.....

(11) local Specify local options

(12) name-server Specify IP address of domain name server to use

.....

Please Input the code of command to be excute(0-20): **11**

Key Word:

Q(quit)

(00)pool IP Local address pool lists

Please Input the code of command to be excute(0-0): **0**

Key Word:

Q(quit)

(00)WORD Create named local address pool

(01)default Create default local address pool

Please Input the code of command to be excute(0-1):**0**

Please input a string:**bdcom** (input username)

Key Word:

Q(quit)

(00)A.B.C.D Set first IP address and Number of IP addresses of pool

Please Input the code of command to be excute(0-0): **0**

Please input a string:Please input a IP address:**10.0.0.1** (input ip address)

Key Word:

Q(quit)

(00)<1 - 1024> Number of IP addresses of pool

(01)<cr> default is 1

Please Input the code of command to be excute(0-1):**0**

Please input a string:**10** (input Number of IP pool)

Key Word:

Q(quit)

(00)<cr>

Please Input the code of command to be excute(0-0):**0**

Will you excute it? (Y/N):**y**

[DEFAULT@Router /config/#**interface**

(00)FastEthernet FastEthernet interface

(01)Serial Serial interface

(02)Async Asynchronous interface

.....

Please Input the code of command to be excute(0-9): **2**

Please input a interface name:**s0/1** ( input the interface name )

Will you excute it? (Y/N):**y**

Key Word:

Q(quit)

.....  
 (26)physical-layer                      Configure physical layer parameters  
 (27)ppp                                      Point-to-point protocol

.....  
 Please Input the code of command to be excute(0-35): 27

Key Word:

U(undo)    D(default)                      Q(quit)  
 (00)default                                      Specify default parameters

(01)neighbor-route                      Create neighbor route to peer if needed

Please Input the code of command to be excute(0-1): 0

(00)ip    Specify default IP parameters

Please Input the code of command to be excute(0-0): 0

(00)address                                      Specify default IP address

Please Input the code of command to be excute(0-0): 0

(00)A.B.C.D                                      Default IP address for remote end of this

interface

(01)dhcp    Use DHCP proxy client to allocate a peer IP

address

(02)pool    Use IP pool mechanism to allocate a peer IP address

Please Input the code of command to be excute(0-2):2

(00)WORD    Name of IP address local-pool

Please Input the code of command to be excute(0-0): 0

Please input a string:**D-link**    ( input the ip pool name , the string "D-link" here is just for example )

Will you excute it? (Y/N):y

To define an IP address for a specified interface, use the following commands:

Command	Purpose
<b>ip local pool</b> <i>poolname</i> { <i>begin-ip-address</i> [ <i>ip-address-number</i> ] }	Creates one or more local IP address pools.
<b>interface</b> <i>type number</i>	Specifies the interface and enters interface configuration mode.
<b>peer default config-ip</b> <i>addr</i> <i>ip-address</i>	Specifies the specified address.

Key Word:

U(undo)                      D(default)                      Q(quit)

.....  
 (25)peer    Peer parameters for point to point interfaces

(26)physical-layer                      Configure physical layer parameters

.....  
 Please Input the code of command to be excute(0-35): 25

Key Word:

U(undo)    D(default)                      Q(quit)  
 (00)default                                      Specify default parameters

(01)neighbor-route                      Create neighbor route to peer if needed

Please Input the code of command to be excute(0-1): 0

Key Word:

Q(quit)

```
(00)ip                               Specify default IP parameters
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)address                           Specify default IP address
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)A.B.C.D                           Default IP address for remote end of this interface
(01)dhcp                               Use DHCP proxy client to allocate a peer IP address
(02)pool                               Use IP pool mechanism to allocate a peer IP address
Please Input the code of command to be excute(0-2): 0
Please input a IP Address:192.168.0.1 ( input ip address )
Will you excute it? (Y/N):y
```

#### 4.5.11 Disabling or Reenabling Peer Host Routes

The D-Link router automatically creates neighbor routes by default; that is, it automatically sets up a route to the peer address on a point-to-point interface when the PPP IPCP negotiation is completed.

To disable this default behavior, or to reenale it once it has been disabled, use the following commands in interface configuration mode:

Command	Purpose
<b>peer (undo) neighbor-route</b>	Disables creation of neighbor routes.
<b>peer neighbor-route</b>	Reenables creation of neighbor routes.

Key Word:

```
Q(quit)
.....
(24)pdp                               pdp configuration commands
(25)peer                               Peer parameters for point to point interfaces
.....
Please Input the code of command to be excute(0-35): 25
Key Word:
U(undo)  D(default)                  Q(quit)
(00)default                           Specify default parameters
(01)neighbor-route                    Create neighbor route to peer if needed
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y
```

#### 4.5.12 Configuring Multilink PPP

The Multilink PPP feature provides load balancing functionality over multiple WAN links. The D-Link implementation of The Multilink PPP supports the fragmentation and packet sequencing specifications in RFC 1717.

The Multilink PPP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address. The multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound traffic, outbound traffic, or on either, as needed for the traffic between the specific sites. The Multilink PPP provides bandwidth on demand and reduces transmission latency across WAN links.

The Multilink PPP is designed to work over the following types of single or multiple interfaces:

1. Synchronous or Asynchronous serial interfaces
2. BRI interfaces
3. PRI interfaces

#### 4.5.13 Configuring Multilink PPP on Dialing Line

For example, to configure Multilink PPP on synchronous interfaces, firstly your interface must support dialer and PPP encapsulation, and then you configure a dialer interfaces to support PPP encapsulation and Multilink PPP.

To configure a synchronous interface, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<b>interface async</b> <i>number</i>	Specifies an asynchronous interface.
2	<b>ip (undo) address</b>	Specifies no IP address for the interface.
3	<b>config-encap ppp</b>	Enables PPP encapsulation.
4	<b>line dial</b>	Enables dialing on the interface.
5	<b>dialer rotary-group</b> <i>number</i>	Includes the interface in a specific dialer group.

[DEFAULT@Router /config/#**interface**

Key Word:

U(undo)                    D(default)                    Q(quit)

.....

(02)Serial                                    Serial interface

(03)Async                                    Asynchronous interface

.....

Please Input the code of command to be excute(0-11): **3**

Please input a interface name:**a0/0** ( input interface name )

Will you excute it? (Y/N):**y**

Key Word:

Q(quit)

.....

(19)ip                                        IP configuration commands

(20)line                                      Configure dialing mode

.....

Please Input the code of command to be excute(0-35): **19**

Key Word:

U(undo)    D(default)                    Q(quit)

(00)access-group                            Specify access control for packets

(01)address                                 IP address

.....

Please Input the code of command to be excute(0-18): **u**

Key Word:

U(undo)    D(default)                    Q(quit)

(00)access-group                            Specify access control for packets

(01)address                                 IP address

.....

Please Input the code of command to be excute(0-18): **1**

Key Word:

Q(quit)

(00)A.B.C.D                                 IP address

(01)negotiated                              IP address negotiated over PPP or via DHCP

(02)<cr>

Please Input the code of command to be excute(0-2): **2**

Will you excute it? (Y/N):**y**

Key Word:

Q(quit)

.....

(08)dsr-ignore ignore dsr signal

(09)encapsulation Set encapsulation type for an interface

.....

Please Input the code of command to be excute(0-25): **9**

Key Word:

U(undo) D(default) Q(quit)

(00)ppp PPP Protocol

(01)<cr>

Please Input the code of command to be excute(0-1): **0**

Will you excute it? (Y/N):**y**

Key Word:

Q(quit)

.....

(19)ip IP configuration commands

(20)line Configure dialing mode

.....

Please Input the code of command to be excute(0-35): **20**

Key Word:

U(undo) D(default) Q(quit)

(00)dial Set dial-line

(01)leased Set leased-line

Please Input the code of command to be excute(0-1): **0**

Will you excute it? (Y/N):**y**

Key Word:

Q(quit)

.....

(11)dialer Dial-on-demand routing (DDR) commands

(12)dialer-group Assign interface to dialer-list

.....

Please Input the code of command to be excute(0-38): **11**

Key Word:

U(undo) D(default) Q(quit)

.....

(08)priority Set interface priority in dialer rotary group

(09)rotary-group Add this interface to a dialer rotary group

.....

Please Input the code of command to be excute(0-11): **9**

Key Word:

Q(quit)

(00)Dialer Dialer interface

Please Input the code of command to be excute(0-0): **0**

Please input a interface name:**d1** ( input Dialer interface )

Will you excute it? (Y/N):**y**

Repeat these steps for additional synchronous interfaces, if it's needed.

**Note: To configure set-dialer rotary-group interface, the PPP configuration will automatic synchronize with corresponding dialer interface**

To configure a dialer interface, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<b>interface dialer</b> <i>number</i>	Define a dialer rotary group
2	<b>ip (undo) address</b>	Specifies no IP address for the interface.
3	<b>dialer load-threshold</b> <i>load</i>	Specifies the dialer load threshold for bringing up additional WAN links.
4	<b>ppp multi-link</b>	Enable Multilink PPP.

For example:

```
[DEFAULT@Router /config/]#interface
```

Key Word:

```
U(undo)  D(default)      Q(quit)
```

.....

```
(08)Dialer                      Dialer interface
```

```
(09)Multilink                   Multilink-group interface
```

.....

```
Please Input the code of command to be excute(0-11): 8
```

```
Please input a interface name:dl ( input dialer interface )
```

```
Will you excute it? (Y/N):y
```

Key Word:

```
Q(quit)
```

.....

```
(15)ip                          IP configuration commands
```

```
(16)mtu                          Set the interface MTU
```

.....

```
Please Input the code of command to be excute(0-28): 15
```

Key Word:

```
U(undo)  D(default)      Q(quit)
```

```
(00)access-group                Specify access control for packets
```

```
(01)address                     IP address
```

.....

```
Please Input the code of command to be excute(0-18): u
```

Key Word:

```
U(undo)  D(default)      Q(quit)
```

```
(00)access-group                Specify access control for packets
```

```
(01)address                     IP address
```

.....

```
Please Input the code of command to be excute(0-18): 1
```

Key Word:

```
Q(quit)
```

```
(00)A.B.C.D                     IP address
```

```
(01)negotiated                  IP address negotiated over PPP or via DHCP
```

```
(02)<cr>
```

```
Please Input the code of command to be excute(0-2): 2
```

```
Will you excute it? (Y/N):y
```

Key Word:

```

Q(quit)
.....
(08)dialer                               Dial-on-demand routing (DDR) commands
(09)dialer-group                          Assign interface to dialer-list
.....
Please Input the code of command to be excute(0-28): 8
Key Word:
U(undo)  D(default)          Q(quit)
.....
(06)load-threshold            Specify threshold for placing additional calls
(07)map                       Define multiple dial-on-demand numbers
.....
Please Input the code of command to be excute(0-11): 6
Key Word:
Q(quit)
(00)<0-100>                    Load threshold to place another call
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:50 ( input threshold value )
Key Word:
Q(quit)
(00)<0-100>                    Load threshold to disconnect a call
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:100 ( input threshold value )
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(21)peer                        Peer parameters for point to point interfaces
(22)ppp                         Point-to-point protocol
.....
Please Input the code of command to be excute(0-28): 22
Key Word:
U(undo)  D(default)          Q(quit)
.....
(07)multilink                  Make interface multilink capable
(08)pap                        Set PAP authentication parameters
(09)timeout                    Set PPP timeout parameters
Please Input the code of command to be excute(0-9): 7
Will you excute it? (Y/N):y

```

#### 4.5.14 Configuring MLP on a Single ISDN BRI Interface

To enable MLP on a single ISDN BRI interface, you are not required to define a **dialer rotary** group separately because ISDN interfaces are **dialer rotary** groups by default.

To configure an ISDN BRI interface, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<b>interface bri number</b>	Define an interface
2	<b>ip addr</b> <i>ip-address mask</i> [ <b>secondary</b> ]	Specify an appropriate protocol address.
3	<b>encapsulation ppp</b>	Enable PPP encapsulation

4	<b>dialer idle-timeout</b> <i>seconds</i>	(Optional) Specifies a dialer idle timeout.
5	<b>dialer load-threshold</b> <i>load</i>	Specifies the dialer load threshold for bringing up additional WAN links.
6	<b>dialer map</b> <i>protocol next-hop-address</i> [ <b>name</b> <i>hostname</i> ] [ <b>broadcast</b> ] [ <i>dial-string[:isdn-subaddress]</i> ]	Configure dialer map
7	<b>dialer-group</b> <i>group-number</i>	Controls access to this interface by adding it to a <b>dialer access</b> group.
8	<b>ppp authentication</b> [ <b>pap chap ms-chap</b> ]	(Optional) Enables PPP authentication.
9	<b>ppp multi-link</b>	Enable Multilink PPP.

**For example:**

```
[DEFAULT@Router /b2/0/]#interface
```

```
.....
```

```
(04)BRI                               ISDN Basic Rate Interface
```

```
(05)Null                               Null interface
```

```
.....
```

```
Please Input the code of command to be excute(0-11): 4
```

```
Please input a interface name:bri 2/0 ( input the interface name , here is just an example )
```

```
Will you excute it? (Y/N):y
```

```
Key Word:
```

```
Q(quit)
```

```
.....
```

```
(18)interface                         interface configuration
```

```
(19)ip                                 IP configuration commands
```

```
.....
```

```
Please Input the code of command to be excute(0-32): 19
```

```
Key Word:
```

```
U(undo)          D(default)          Q(quit)
```

```
(00)access-group Specify access control for packets
```

```
(01)address      IP address
```

```
.....
```

```
Please Input the code of command to be excute(0-18): 1
```

```
(00)A.B.C.D      IP address
```

```
(01)negotiated  IP address negotiated over PPP or via DHCP
```

```
Please Input the code of command to be excute(0-1): 0
```

```
Please input a IP Address:192.168.0.1 255.255.255.0 ( input ip address , this is just an example )
```

```
(00)secondary      Make this IP address a secondary address
```

```
(01)<cr>
```

```
Please Input the code of command to be excute(0-1): 1
```

```
Will you excute it? (Y/N):y
```

```
Key Word:
```

```
U(undo)          D(default)          Q(quit)
```

```
.....
```

```
(11)dialer-group Assign interface to dialer-list
```

```
(12)encapsulation Set encapsulation type for an interface
```

```
.....
```

```
Please Input the code of command to be excute(0-32): 12
```

```
Key Word:
```

```
U(undo)          D(default)          Q(quit)
```

```

(00)ppp                                     PPP Protocol
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y
Key Word:
U(undo)          D(default)          Q(quit)
.....
(09)description          Set the interface description
(10)dialer             Dial-on-demand routing (DDR) commands
.....
Please Input the code of command to be excute(0-32): 10
Key Word:
U(undo)          D(default)          Q(quit)
.....
(04)hold-queue          Set output hold queue length
(05)idle-timeout        Set idle time before disconnecting line
.....
Please Input the code of command to be excute(0-11): 5
(00)<0-2147483>          Idle timeout in seconds
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:300 ( input idle-timeout time , this is just an example )
Will you excute it? (Y/N):y
Key Word:
U(undo)          D(default)          Q(quit)
.....
(09)description          Set the interface description
(10)dialer             Dial-on-demand routing (DDR) commands
.....
Please Input the code of command to be excute(0-32): 10
Key Word:
U(undo)          D(default)          Q(quit)
.....
(05)idle-timeout        Set idle time before disconnecting line
(06)load-threshold      Specify threshold for placing additional calls
.....
Please Input the code of command to be excute(0-11): 6
(00)<0-100>              Load threshold to place another call
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:500 ( input Load threshold , this is just an example )
Will you excute it? (Y/N):y
Key Word:
U(undo)          D(default)          Q(quit)
.....
(09)description          Set the interface description
(10)dialer             Dial-on-demand routing (DDR) commands
.....
Please Input the code of command to be excute(0-32): 10
Key Word:
U(undo)          D(default)          Q(quit)
.....

```

```

(07)map                Define multiple dial-on-demand numbers
(08)remote-name        Specify remote name
Please Input the code of command to be excute(0-11): 7
(00)A.B.C.D                IP address
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:192.168.1.2 ( input ip address , this is just an example )
.....
(04)name                Map to a host
(05)system-script        Specify system dialing script
Please Input the code of command to be excute(0-5): 4
(00)WORD                Host name to map
Please Input the code of command to be excute(0-0): 0
Please input a string:router ( input the host name , this is just an example )
(00)WORD                Dialer string
(01)broadcast            Broadcast to this address
.....
Please Input the code of command to be excute(0-4): 1
(00)WORD                Dialer string
(01)class                Dialer map class
.....
Please Input the code of command to be excute(0-3): 0
Please input a string:1234 ( input dial-string , this is just an example )
Will you excute it? (Y/N):y
Key Word:
U(undo)                D(default)                Q(quit)
.....
(10)dialer                Dial-on-demand routing (DDR) commands
(11)dialer-group          Assign interface to dialer-list
.....
Please Input the code of command to be excute(0-32): 11
Key Word:
U(undo)                D(default)                Q(quit)
(00)<1-10>                Dialer list number
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:5 ( input dial list number , this is just an example )
Will you excute it? (Y/N):y
Key Word:
U(undo)                D(default)                Q(quit)
.....
(23)peer                Peer parameters for point to point interfaces
(24)ppp                Point-to-point protocol
.....
Please Input the code of command to be excute(0-32): 24
Key Word:
U(undo)                D(default)                Q(quit)
(00)authentication        Set PPP link authentication method
(01)authorization        Set PPP network authorization method
.....
Please Input the code of command to be excute(0-9): 0

```

```

(00)chap                Challenge Handshake Authentication Protocol (CHAP)
(01)ms-chap             Microsoft Challenge Handshake Authentication Protocol(MS-CHAP)
(02)pap                 Password Authentication Protocol (PAP)
Please Input the code of command to be excute(0-2): 0
(00)WORD                Use an authentication list with this name
.....
(04)pap                 Password Authentication Protocol (PAP)
(05)<cr>
Please Input the code of command to be excute(0-5): 5
Will you excute it? (Y/N):y
Key Word:
U(undo)                D(default)                Q(quit)
.....
(23)peer                Peer parameters for point to point interfaces
(24)ppp                 Point-to-point protocol
.....
Please Input the code of command to be excute(0-32): 24
Key Word:
U(undo)                D(default)                Q(quit)
.....
(07)multilink           Make interface multilink capable
(08)pap                 Set PAP authentication parameters
(09)timeout             Set PPP timeout parameters
Please Input the code of command to be excute(0-9): 7
Will you excute it? (Y/N):y

```

#### 4.5.15 Configuring MLP on Multiple ISDN BRI Interfaces

To enable MLP on multiple ISDN BRI interfaces, set up a dialer rotary interface and configure it for Multilink PPP, then configure the BRI interfaces separately and add them to the same **rotary** group.

To set up the dialer rotary interface, use the following commands:

Step	Command	Purpose
1	<b>interface dialer</b> <i>number</i>	Define an interface
2	<b>ip address</b> <i>ip-address mask</i>	Specify an appropriate IP address.
3	<b>encapsulation ppp</b>	Enable PPP encapsulation
4	<b>dialer idle-timeout</b> <i>seconds</i>	(Optional) Specifies the <b>dialer idle</b> timeout period.
5	<b>dialer load-threshold</b> <i>load</i>	Configure the maximum load threshold specified by the dialer.
6	<b>dialer map</b> <i>protocol next-hop-address</i> [ <b>name</b> <i>hostname</i> ] [ <b>broadcast</b> ] [ <i>dial-string[:isdn-subaddress]</i> ]	Configure dialer map
7	<b>dialer-group</b> <i>group-number</i>	Controls access to this interface by adding it to a <b>dialer access</b> group.
8	<b>ppp authentication</b> [ <b>pap chap ms-chap</b> ]	(Optional) Enables PPP authentication.
9	<b>ppp multilink</b>	Enable Multilink PPP.

[DEFAULT@Router /config/]#**interface**

.....

```

(08)Dialer                               Dialer interface
(09)Multilink                             Multilink-group interface
(10)Virtual-template                       Virtual template interface
(11)Virtual-tunnel                         Virtual tunnel interface
Please Input the code of command to be excute(0-11): 8
Please input a interface name:d1 ( input dialer interface name , this is just an example )
Will you excute it? (Y/N):y
Key Word:
      U(undo)           D(default)           Q(quit)
      .....
(19)ip                               IP configuration commands
(20)mtu                             Set the interface MTU
.....
Please Input the code of command to be excute(0-32): 19
Key Word:
      U(undo)           D(default)           Q(quit)
(00)access-group       Specify access control for packets
(01)address            IP address
(02)beigrp             Enhanced Interior Gateway Routing Protocol
      .....
Please Input the code of command to be excute(0-18): 1
(00)A.B.C.D            IP address
(01)negotiated        IP address negotiated over PPP or via DHCP
Please Input the code of command to be excute(0-1): 0
Please input a IP Address:192.168.1.1 255.255.255.0 ( input ip address , this is just an example )
(00)secondary        Make this IP address a secondary address
(01)<cr>
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y
Key Word:
      U(undo)           D(default)           Q(quit)
      .....
(12)encapsulation     Set encapsulation type for an interface
(13)english           help message in English
.....
Please Input the code of command to be excute(0-32): 12
Key Word:
      U(undo)           D(default)           Q(quit)
(00)ppp               PPP Protocol
Please Input the code of command to be excute(0-0): 0
      Will you excute it? (Y/N):y
Key Word:
      U(undo)           D(default)           Q(quit)
      .....
(10)dialer            Dial-on-demand routing (DDR) commands
(11)dialer-group      Assign interface to dialer-list
.....
Please Input the code of command to be excute(0-32): 10
Key Word:

```

```

                U(undo)          D(default)          Q(quit)
.....
(04)hold-queue          Set output hold queue length
(05)idle-timeout       Set idle time before disconnecting line
.....
Please Input the code of command to be excute(0-11): 0
(00)<0-2147483>                               Idle timeout in seconds
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:300 ( input idle-timeout , this is just an example )
Will you excute it? (Y/N):y
Key Word:
                U(undo)          D(default)          Q(quit)
.....
                (10)dialer          Dial-on-demand routing (DDR) commands
                (11)dialer-group    Assign interface to dialer-list
.....
Please Input the code of command to be excute(0-32): 10
Key Word:
                U(undo)          D(default)          Q(quit)
.....
(05)idle-timeout       Set idle time before disconnecting line
                (06)load-threshold    Specify threshold for placing additional calls
.....
Please Input the code of command to be excute(0-11): 6
                (00)<0-100>          Load threshold to place another call
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:50 ( input threshold , this is just an example )
                (00)<0-100>          Load threshold to disconnect a call
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:30 ( input threshold , this is just an example )
Will you excute it? (Y/N):y
Key Word:
                U(undo)          D(default)          Q(quit)
.....
(10)dialer          Dial-on-demand routing (DDR) commands
(11)dialer-group    Assign interface to dialer-list
.....
Please Input the code of command to be excute(0-32): 10
Key Word:
                U(undo)          D(default)          Q(quit)
(00)called          Dialer called string
.....
(06)load-threshold    Specify threshold for placing additional calls
(07)map              Define multiple dial-on-demand numbers
.....
Please Input the code of command to be excute(0-11): 7
(00)A.B.C.D          IP address
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:192.168.1.2 ( input ip address , this is just an example )

```



Key Word:

U(undo)                      D(default)                      Q(quit)

.....

(07)multilink                      Make interface multilink capable  
 (08)pap                      Set PAP authentication parameters  
 (09)timeout                      Set PPP timeout parameters

Please Input the code of command to be excute(0-9): 7

Will you excute it? (Y/N):y

To configure the BRI interfaces to belong to the **dialer rotary** group, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<b>interface bri</b> <i>number</i>	Specifies an interfaces.
2	<b>ip (undo) addr</b>	Do not configure IP address
3	<b>encapsulation ppp</b>	Enable PPP encapsulation
4	<b>dialer idle-timeout</b> <i>seconds</i>	(Optional)Sets the dialer idle timeout period
5	<b>dialer rotary-group</b> <i>number</i>	Adds the interface to the dialer rotary group.
6	<b>dialer load-threshold</b> <i>load</i>	Configure the maximum load threshold of dialer

[DEFAULT@Router /config/]#**interface**.....

(03)AsyncAsynchronous interface

(04)BRIISDN Basic Rate Interface.....

Please Input the code of command to be excute(0-11):4

Please input a interface name:**b2/0** ( input interface name )

Will you excute it? (Y/N):y

Key Word:

U(undo)                      D(default)                      Q(quit)

.....

(19)ipIP                      configuration commands

(20)mtuSet                      the interface MTU

.....

Please Input the code of command to be exc ute(0-32):19

Key Word:

U(undo)                      D(default)                      Q(quit)

(00)access-groupSpecify access control for packets

(01) addressIP address

(02) beigrpEnhanced Interior Gateway Routing Protocol

.....

Please Input the code of command to be excute(0-18):1

(00)A.B.C.DIP address

(01) negotiatedIP address negotiated over PPP or via DHCP

Please Input the code of command to be excute(0-1):0

Please input a IP Address:**192.168.1.1 255.255.255.0**(input ip address)

(00) secondaryMake this IP address a secondary address

(01)<cr>

Please Input the code of command to be excute(0-1):1

Will you excute it? (Y/N):y

Key Word:

U(undo)                      D(default)                      Q(quit)

```

.....
(12)encapsulation      Set encapsulation type for an interface
(13)English           help message in English
.....
Please Input the code of command to be excute(0-32):12
Key Word:
U(undo)      D(default)      Q(quit)
(00)ppp      PPP Protocol
Please Input the code of command to be excute(0-0):0
Will you excute it? (Y/N):y
Key Word:
U(undo)      D(default)      Q(quit)
.....
(10)dialer          Dial-on-demand routing (DDR) commands
(11)dialer-group    Assign interface to dialer-list.....
Please Input the code of command to be excute(0-32):10
Key Word:
U(undo)      D(default)      Q(quit)
.....
(05)idle-timeout    Set idle time before disconnecting line
(06)load-threshold  Specify threshold for placing additional calls
.....
Please Input the code of command to be excute(0-11):5
(00)<0-2147483>      Idle timeout in seconds
Please Input the code of command to be excute(0-0):0
Please input a digital number:Please input a string:300 ( input idle timeout value )
Will you excute it? (Y/N):y
Key Word:
U(undo)D(default)Q(quit)
.....
(10)dialer          Dial-on-demand routing (DDR) commands
(11)dialer-group    Assign interface to dialer-list.....
Please Input the code of command to be excute(0-32):10
Key Word:
U(undo)D(default)Q(quit)
.....
( 09 ) rotary-group  Add this interface to a dialer rotary group
( 10 ) string        Set default telephone number.....
Please Input the code of command to be excute(0-11):11
Key Word:
U(undo)D(default)Q(quit)
.....
( 00 ) DialerDialer interface
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:d1 ( input Dialer interface )
Will you excute it? (Y/N):y

```

Repeat Steps 1 through 6 for configure other BRI interfaces.



Will you excute it? (Y/N):y

Key Word:

Q(quit)

.....

(22)ppp Point-to-point protocol

(23)priority-group Assign a priority group to interface

.....

Please Input the code of command to be excute(0-30): **22**

Key Word:

U(undo) D(default) Q(quit)

.....

(04)ipcp Set IPCP parameters

(05)lcp Set LCP parameters

.....

Please Input the code of command to be excute(0-9): **5**

Key Word:

Q(quit)

.....

(04)open Open LCP connection

(05)enddisc-type Select enddisc type

Please Input the code of command to be excute(0-5): **5**

Key Word:

Q(quit) Null class

(00)null Null class

(01)local Locally Assigned Address

.....

Please Input the code of command to be excute(0-5): **1**

Will you excute it? (Y/N):y

Key Word:

Q(quit)

.....

(21)peer Peer parameters for point to point interfaces

(22)ppp Point-to-point protocol

.....

Please Input the code of command to be excute(0-30): **22**

Key Word:

U(undo) D(default) Q(quit)

(00)authentication Set PPP link authentication method

(01)authorization Set PPP network authorization method

.....

Please Input the code of command to be excute(0-9): **0**

Key Word:

Q(quit)

(00)chap Challenge Handshake Authentication Protocol (CHAP)

(01)ms-chap Microsoft Challenge Handshake Authentication

Protocol(MS-CHAP)

(02)pap Password Authentication Protocol (PAP)

Please Input the code of command to be excute(0-2): **0**

Key Word:

```

Q(quit)
.....
(04)pap                                Password Authentication Protocol (PAP)
(05)<cr>
Please Input the code of command to be excute(0-5): 5
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(22)ppp                                Point-to-point protocol
(23)priority-group                    Assign a priority group to interface
.....
Please Input the code of command to be excute(0-30): 22
Key Word:
U(undo)          D(default)          Q(quit)
.....
(07)multilink    Make interface multilink capable
(08)pap          Set PAP authentication parameters
(09)timeout     Set PPP timeout parameters
Please Input the code of command to be excute(0-9): 7
Will you excute it? (Y/N):y
<![endif]>

```

Configure the DSL interface belong to multilink group as below:

step	command	function
1	interface type number	Define an interface
2	ip (undo) address	Do not configure IP address
3	encapsulation ppp	Enable PPP encapsulation
4	multilink-group group-number	Add the interface to multilink group

The input order is:

```
[DEFAULT@Router /config/#interface
```

```

(00)FastEthernet    FastEthernet interface
(01)Serial          Serial interface
.....

```

```

Please Input the code of command to be excute(0-9): 1
Please input a interface name:s0/1 ( input the interface name )
Will you excute it? (Y/N):y
Key Word:
U(undo)    D(default)    Q(quit)
.....

```

```

(19)ip                IP configuration commands
(20)mtu              Set the interface MTU
.....

```

Please Input the code of command to be excute(0-32): 19

```

Key Word:
U(undo)    D(default)    Q(quit)
(00)access-group Specify access control for packets
.....

```

Please Input the code of command to be excute(0-18): u

(00)access-group Specify access control for packets  
 (01)address IP address

.....

Please Input the code of command to be excute(0-18): 1

(00)A.B.C.D IP address  
 (01)negotiated IP address negotiated over PPP or via DHCP  
 (02)<cr>

Please Input the code of command to be excute(0-2): 2

Will you excute it? (Y/N):y

Key Word:

U(undo) D(default) Q(quit)

.....

(12)encapsulation Set encapsulation type for an interface  
 (13)english help message in English

.....

Please Input the code of command to be excute(0-32): 12

Key Word:

U(undo) D(default) Q(quit)

(00)frame-relay Frame Relay Protocol  
 (01)hdlc HDLC Protocol  
 (02)ppp PPP Protocol  
 (03)sdlc SDLC Protocol  
 (04)x25 X.25 Protocol

Please Input the code of command to be excute(0-4): 2

Will you excute it? (Y/N):y

Key Word:

U(undo) D(default) Q(quit)

.....

(21)mtu Set the interface MTU  
 (22)multilink-group Put interface in a multilink bundle

.....

Please Input the code of command to be excute(0-35): 22

Key Word:

U(undo) D(default) Q(quit)

(00)<0-32767> Multilink group number

Please Input the code of command to be excute(0-0): 0

Please input a digital number:Please input a string:100 (input the group-number)

Will you excute it? (Y/N):y

Repeat Steps 1 through 4 for configure other DSL interfaces.

**Note: To configure config-multi-link group interface, the PPP configuration will automatic synchronize with corresponding multilink group interface**

#### 4.5.17 PPP Configuration Example

Examples in the following sections section show various PPP configurations:

[CHAP Configuration Example](#)

[Multilink PPP configuration Example](#)

[Configuring MLP on a Single ISDN BRI Interface](#)

[Configuring Multilink PPP on DSL interface](#)

Use virtual-template to Configure multilink**4.5.18 CHAP Configuration Example**

The following configuration examples enable CHAP Authentication Protocol on serial interface 1/0 of two devices.

**Configure the router1**

```
!  
hostname router1  
!  
interface s1/0  
    encapsulation ppp  
    ppp authentication chap  
    ppp chap hostname user1  
!  
username user2 password 0 secret12  
!
```

**configure the router2**

```
!  
hostname router2  
!  
interface s1/0  
    encapsulation ppp  
    ppp authentication chap  
    ppp chap hostname user2  
!  
username user1 password 0 secret12  
!
```

**4.5.19 Multilink PPP Configuration Example**

The following examples configure Multilink PPP. First example is application on one BRI interface, the second apply to configure the DSL interface that belonging to **multilink group** interface, the third example is configuration of **multilink** by **virtual-templat**.

**Multilink PPP on a single ISDN Interface Example**

```
!  
interface bri 0/3  
    description connected to router  
    ip address 192.168.20.100 255.255.255.0  
    encapsulation ppp  
    dialer idle-timeout 30  
    dialer load-threshold 40 either  
    dialer map 171.1.1.8 name router 81012345678901  
    dialer-group 1  
    ppp authentication pap  
    ppp multilink  
!
```

**Multilink PPP on DSL Interface Example**

```
!  
interface multilink 1  
  ip address 192.168.20.100 255.0.0.0  
  encapsulation ppp  
  ppp lcp enddisc-type local  
  ppp authentication chap  
  ppp chap hostname router  
  ppp multilink  
!  
interface s1/0  
  ip (undo) address  
  encapsulation ppp  
  ppp lcp enddisc-type local  
  ppp authentication chap  
  ppp chap hostname router  
  ppp multilink  
  multilink-gourp 1  
!  
interface s1/1  
  ip (undo) address  
  encapsulation ppp  
  ppp lcp enddisc-type local  
  ppp authentication chap  
  ppp chap hostname router  
  ppp multilink  
  multilink-gourp 1  
!  
interface s1/2  
  ip (undo) address  
  encapsulation ppp  
  ppp lcp enddisc-type local  
  ppp authentication chap  
  ppp chap hostname router  
  ppp multilink  
  multilink-gourp 1  
!
```

**Use virtual-template to Configure multilink**

```
!  
multilink virtual-template 1  
!  
interface virtual-template 1  
  ip address 192.168.20.100  
  ppp lcp enddisc-type ppp  
  ppp multilink  
!  
interface s1/0
```

```

physical-layer mode async
ip (undo) address
ip (undo) directed-broadcast
ppp lcp enddisc-type ppp
ppp authentication pap
ppp multilink
ppp pap sent-username router mypassword
physical-layer speed 57600
!
interface s1/1
physical-layer mode async
ip (undo) address
ip (undo) directed-broadcast
ppp lcp enddisc-type ppp
ppp authentication pap
ppp multilink
ppp pap sent-username router mypassword
physical-layer speed 57600
!
```

#### 4.5.20 PPPoE Client Illustration

D-Link router supports PPPoE Client end to establish PPP connection with Access Server through Ethernet or ADSL high speed line and provides PPP correlative authentication, accounting and authorization.

##### PPPoE Software configuration

This section describes how to configure PPPoE Client on router. Please see [“PPPoE Configuring Command”](#) for more details.

##### PPPoE Configuration Task List

D-Link router can establish PPP connection with remote Access Server through Ethernet. User must perform the following tasks:

- 1)Configure dial interface;
- 2)Configure PPPoE features.

To understand the configuration of PPPoE, refer to [“PPPoE Configuration Example”](#) section at the end of the chapter. Please see the [“WANs Command Reference”](#) to get the introduction of PPP commands. For the detailed information of link layer, network layer protocol and router protocol configuration, please see the correlative chapters.

##### PPPoE Configuring Command List

Global Configuration Command

**interface dialer** *number* ;

Interface Configuration Command

4. 1. Configure the PPP protocol correlated configuration on established Dialer interface(see the description of Dialer interface configuration and PPP protocol configuration.)  
(Note: as the restriction of Ethernet message length, PPP protocol header will take up fixed spending, therefore, user must performs the CONFIG-IP MTU 1492 command on this interface)
5. 2. configuring on Ethernet port that loaded the PPP protocol.  
pppoe-client dialer number

#### 4.5.21 PPPoE Client Configuration Example

Following describes the typical application environment of PPPoE.

The router connects with multiple hosts over Ethernet interface Ethernet1/1, and connects with ADSL Modem through the interface Ethernet2/0. The router creates PPP connection with Access Server and implements that multiple hosts(192.168.20.0 net segment) simultanerty connect to network at one time by Nat feature.

Configuration is given below:

```
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip (undo) directed-broadcast
 ppp pap sent-username 8888 888
 ip nat outside
!
interface Ethernet1/1
 ip address 192.168.20.1 255.255.255.0
 ip (undo) directed-broadcast
 ip nat inside
!
interface Ethernet2/0
 ip (undo) address
 ip (undo) directed-broadcast
 pppoe-client Dialer1
!
!
ip route default Dialer1
!
ip access-list standard 1
 permit 192.168.0.0 255.255.0.0
!
!
!
ip nat inside source list 1 interface Dialer1
!
!
!
```

## 4.6 Configuring SLIP Task List

### 4.6.1 Implementation Information

SLIP protocol provides the method that encapsulate the network layer protocol information on point-to-point connection. This protocol can be configured on the following types of physical interface:

Asynchronous Serial Interface

### 4.6.2 SLIP Configuration Task List

To configure the SLIP on asynchronous serial interface(if it was synchronous, you should use the command “physical-layer mode async” to change it into asynchronous mode), perform the following task in interface configuration mode:

Enable SLIP encapsulation

### 4.6.3 Enable SLIP Encapsulation

To encapsulate the IP packet, encapsulate the SLIP protocol on serial line.

Command	Purpose
<b>encapsulation slip</b>	Enable SLIP encapsulation.

Key Word:

```
U(undo) D(default) Q(quit)
.....
(11)dsr-ignore ignore dsr signal
(12)encapsulation Set encapsulation type for an interface
(13)english help message in English
.....
```

Please Input the code of command to be excute(0-35): **12**

Key Word:

```
U(undo) D(default) Q(quit)
(00)ppp PPP Protocol
(01)slip SLIP Protocol
```

Please Input the code of command to be excute(0-1): **1**

Will you excute it? (Y/N):y

## 4.7 Configuring HDLC Task List

### 4.7.1 Implementation Information

HDLC protocol provides the method that encapsulate the network layer protocol information on point-to-point connection. This protocol can be configured on the following types of physical interface:

- ? ISDN
- ? Synchronous Serial Interface

### 4.7.2 HDLC Confiureation Task List

To configure the HDLC on serial interface(include ISDN), perform the following task in interface configuration mode:

Enable HDLC Encapsulation

### 4.7.3 Enable HDLC Encapsulation

To encapsulate the IP packet, encapsulate the SLIP protocol on serial line.

Command	Purpose
<b>encapsulation hdlc</b>	Enable HDLC encapsulation.

Implementing the following configuration in the interface configurative mode:

Key Word:

```
U(undo) D(default) Q(quit)
.....
(11)encapsulation Set encapsulation type for an interface
(12)english help message in English
.....
```

Please Input the code of command to be excute(0-30): **11**

Key Word:

```
U(undo) D(default) Q(quit)
(00)frame-relay Frame Relay Protocol
```

```
(01)hdlc                                HDLC Protocol
```

```
.....
```

```
Please Input the code of command to be excute(0-4): 1
```

```
Will you excute it? (Y/N):y
```

#### 4.8 Configuring ISDN BRI Task List

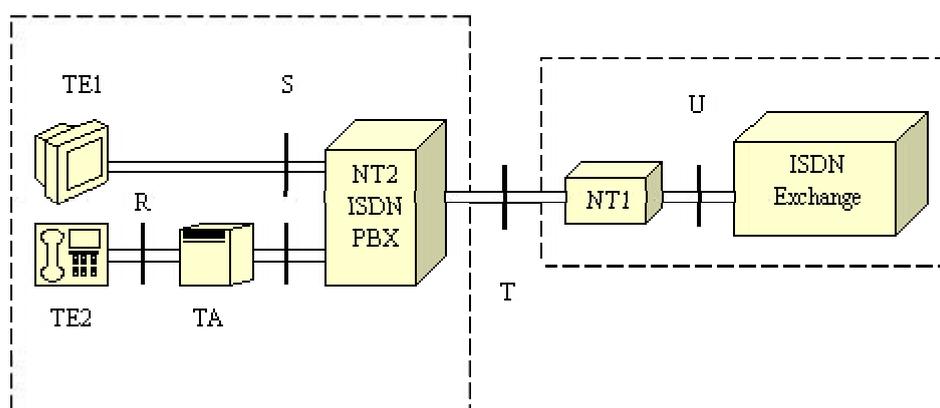
##### ISDN

Integrated Services Digital Network(ISDN) is new and developing technology growing since 1970s, which provides entire digital service form end user to another end use. ISDN implemented the entire digital transferring mode includes voice, data, image, and video, etc.

ISDN is different from the traditional PSTN network. The user information in the traditional PTSN network send to switch through the analog user loop and convert to digital signal by A/D. Then, the digital signal is transmitted to target user through the digital exchange and transmitting network and revert to analog signal. ISDN solve the the digital transmission of user loop and implement the digitalization of end-to-end. In addition, user can solve the transferring of various digital signal and analog signal through the standardized digital interface. Furthermore, ITU-T established ISDN operating criterion associate with standardization to realize the integrated services. ITU-T also established the protocols that include I.430, Q.921 and Q.931, etc. Thus, all the deveices that accord with physical interfaces and software protocols can be connected with ISDN network smoothly.

ISDN BRI provides two B channels, each capable of transferring voice or data at 64 kbps, and one 16-kbps D channel that carries signaling traffic. You can configure each B channel as a single port. The aggregate of ISDN signaling channel can be executed by multi-link feature, which is to combine multiple physical links into a logical beam. This aggregate of link can increase the bandwidth of connecting. In addition, ISDN BRI can dynamic assign various links to make the ISDN line available while it is needed. This setting can eliminate the excrescent bandwidth and increase the utilizing efficiency of user.

ITU-T I.411 advice bringup the referenced configuration of ISDN user-network interface accord to the concept of fuction group (a group of functions that the user needed while connect to ISDN), reference point (use for distinguish the points of the function group concept), shown as below:



The function group are divided as:

- network terminal 1(NT1): implement the function of OSI layer one,including the transmit function of user's line , loop-back function and channel D competition and so on
- network terminal 2(NT2): also called as intelligent terminal
- terminal equipment 1(TE1): Also called as ISDN standard terminal, an user device (such as digital phone) which conforms to ISDN interface standard.
- terminla equipment 2(TE2): Also called as non-ISDN standard terminal, an user device which does not conform to the ISDN interface standard

- terminal adaptor(TA): Implement the function of adapt, connect TE2 to ISDN standard interface.

The reference points include:

- reference point R: between TA and non-ISDN standard terminal equipment
- reference point S: between NT2 and user terminal
- reference point T: between NT1 and NT2
- reference point U: between NT1 and line terminal equipment

According to the difference of regions ,the ISDN switch can be divided into several types: Europe,North America,Australia, Japan and so on. The protocols they conformed to have many difference. However ,the ISDN switch of different manufacturer keeps good compatibility between each other. Therefore, even if the local BRI uses different types of switch with remote end, it will not obstruct the normal operation of the call.you can use the command “config-isdn switch-type” to set the type of ISDN switch which connects with your BRI interface.

TEI negotiation has two types: one is execute it at calling, another is to use the command “isdn tei-negotiation” to configure the ISDN TEI-negotiation.

About ISDN BRI configuration commands, see also “ISDN commands”.

#### 4.8.1 ISDN BRI Interface Configuration Task List

The default data-link-layer protocol of ISDN BRI interface is PPP. To implement IP protocol on the ISDN BRI interface, you need to do the following configurations:

- set ISDN parameters
- set the IP address of an ISDN BRI interface or enable the address negotiation
- set the Dialer map to the destination address
- set the data-link-layer protocol PPP and its authentication
- set DDR parameters
- set related IP route

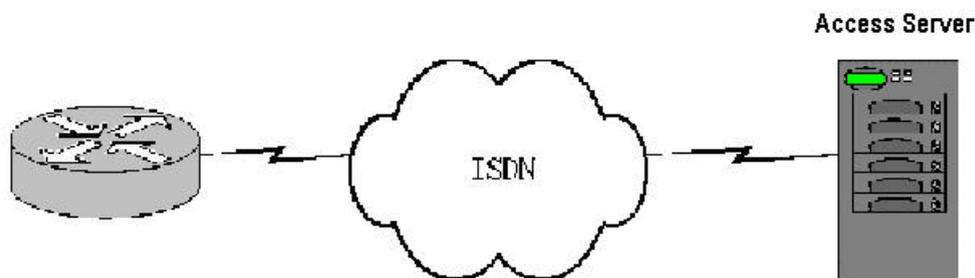
Refer to the related configuration command for more detail of these settings.

#### 4.8.2 ISDN BRI Interface Configuration Examples

1. Example 1: connect with the internet through ISDN , the remote is access server

a. Network requirement: D-LINK 1700 router interconnects with access server through the ISDN BRI interface and implement IP network protocol.

b. Figure



c. Configuration step

configure the ISDN BRI interface of D-LINK 1750 router:

```
[DEFAULT@Router /config/]#isdn
```

(00)switch-type	Select the ISDN switch type
(01)tei-negotiation	Set when ISDN TEI negotiation should occur
Please Input the code of command to be excute(0-1): 0	
(00)basic -1tr6	1TR6 switch type for Germany
(01)basic -5ess	AT&T 5ESS switch type for the U.S.



Key Word:

U(undo) D(default) Q(quit)

.....

(18)interface interface configuration

(19)ip IP configuration commands

.....

Please Input the code of command to be excute(0-32): **19**

Key Word:

U(undo) D(default) Q(quit)

(00)access-group Specify access control for packets

(01)address IP address

.....

Please Input the code of command to be excute(0-18): **1**

(00)A.B.C.D IP address

(01)negotiated IP address negotiated over PPP or via DHCP

Please Input the code of command to be excute(0-1): **1**

Will you excute it? (Y/N):y

### **! configuring the Dialer Map to the NAS**

Key Word:

U(undo) D(default) Q(quit)

.....

(10)dialer Dial-on-demand routing (DDR) commands

(11)dialer-group Assign interface to dialer-list

.....

Please Input the code of command to be excute(0-32): **10**

Key Word:

U(undo) D(default) Q(quit)

.....

(07)map Define multiple dial-on-demand numbers

(08)remote-name Specify remote name

.....

Please Input the code of command to be excute(0-11): **7**

(00)A.B.C.D IP address

Please Input the code of command to be excute(0-0): **0**

Please input a IP Address:**202.96.20.133** ( input ip address )

(00)WORD Dialer string

(01)broadcast Broadcast to this address

.....

Please Input the code of command to be excute(0-5): **0**

Please input a string:**8163** ( input dial-string )

Will you excute it? (Y/N):y

### **! configuring the static route to the NAS**

Key Word:

U(undo) D(default) Q(quit)

.....

(14)exit exit / quit

(15)fair-queue enable fair queue on interface

.....

Please Input the code of command to be excute(0-32): **14**

```

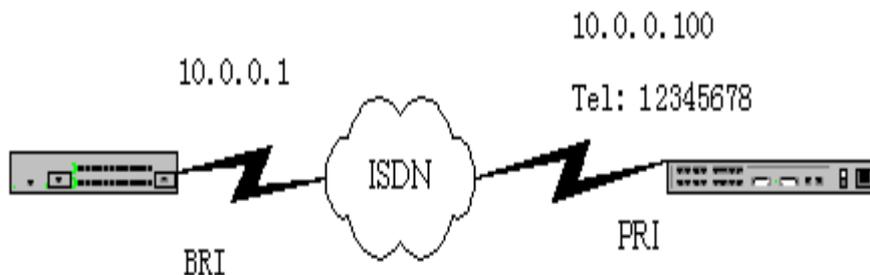
Will you excute it? (Y/N):y
[DEFAULT@Router /config/]#ip
.....
(15)radius                                RADIUS configuration commands
(16)route                                  static route
.....
Please Input the code of command to be excute(0-20): 16
(00)A.B.C.D                                dest IP address
(01)default                                default route
Please Input the code of command to be excute(0-1): 0
Please input a IP Address:0.0.0.0 ( input dest IP address )
(00)A.B.C.D                                dest netmask
Please Input the code of command to be excute(0-0): 00
Please input a IP Address:0.0.0.0 ( input dest netmask )
(00)A.B.C.D                                gateway IP address
(01)interface-name
Please Input the code of command to be excute(0-1): 1
Please input a interface name:b2/0 ( input interface name )
(00)<1-255>                                Distance metric for this route
(01)<cr>
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y

```

## 2. Example 2: Connect local ISDN BRI interface with center ISDN BRI interface

a. network requirement: D-LINK® 1750 router interconnects with the center ISDN PRI interface through ISDN BRI interface which implements IP network protocol.

b. figure



## c. Configuration steps

Configuring the ISDN BRI interface of D-LINK 1750 router:

! configuring the type of global ISDN switch

```

[DEFAULT@Router /config/]#isdn
(00)switch-type                            Select the ISDN switch type
(01)tei-negotiation                        Set when ISDN TEI negotiation should occur
Please Input the code of command to be excute(0-1): 0
(00)basic -1tr6                            1TR6 switch type for Germany
(01)basic -5ess                             AT&T 5ESS switch type for the U.S.
.....
Please Input the code of command to be excute(0-10): 1
Will you excute it? (Y/N):y

```

! configuring the IP address of interface:

```

[DEFAULT@Router /config/]#interface

```



Will you excute it? (Y/N):y

.....

(08)pap Set PAP authentication parameters

(09)timeout Set PPP timeout parameters

Please Input the code of command to be excute(0-9): **8**

(00)refuse Refuse to authenticate using PAP

(01)sent-username Set outbound PAP username and password

Please Input the code of command to be excute(0-1): **1**

(00)WORD Set outbound PAP username and password

Please Input the code of command to be excute(0-0): **0**

Please input a string:**router** ( input username )

(00)WORD Outbound PAP password

Please Input the code of command to be excute(0-0): **0**

Please input a string:**mypassword** ( input password )

Will you excute it? (Y/N):y

! configuring the Dialer Map to the center ISDN PRI

Key Word:

U(undo) D(default) Q(quit)

.....

(10)dialer Dial-on-demand routing (DDR) commands

(11)dialer-group Assign interface to dialer-list

.....

Please Input the code of command to be excute(0-32): **10**

Key Word:

U(undo) D(default) Q(quit)

.....

(07)map Define multiple dial-on-demand numbers

(08)remote-name Specify remote name

.....

Please Input the code of command to be excute(0-11): **7**

(00)A.B.C.D IP address

Please Input the code of command to be excute(0-0): **0**

Please input a IP Address:**10.0.0.100** ( input ip address )

(00)WORD Dialer string

(01)broadcast Broadcast to this address

.....

Please Input the code of command to be excute(0-5): **0**

Please input a string:**12345678** ( input dial-string )

Will you excute it? (Y/N):y

! configuring the static route to the center ISDN PRI

Key Word:

U(undo) D(default) Q(quit)

.....

(14)exit exit / quit

(15)fair-queue enable fair queue on interface

.....

Please Input the code of command to be excute(0-32): **14**

Will you excute it? (Y/N):y

[DEFAULT@Router /config/]#ip

```

.....
(16)route                static route
(17)rsvp                 Configure RSVP information
.....
Please Input the code of command to be excute(0-20): 16
(00)A.B.C.D              dest IP address
(01)default              default route
Please Input the code of command to be excute(0-1): 0
Please input a IP Address:0.0.0.0 ( input dest IP address )
(00)A.B.C.D              dest netmask
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:0.0.0.0 ( input dest mask )
(00)A.B.C.D              gateway IP address
(01)interface-name
Please Input the code of command to be excute(0-1): 1
Please input a interface name:b2/0 ( input interface name )
(00)<1-255>              Distance metric for this route
(01)<cr>
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y

```

#### 4.9 configuring WAN performance

##### Implementation information

Fast-switch provides that the router can switch the IP packets directly to the physical port of routing next hop without passing through the IP layer. This function can be configured on the interface which has encapsulated PPP ,HDLC or ARP protocol.

##### Fast-switch configurative task list

The tasks of configuring fast switch are illustrated below:

##### Configuring the enable of global fast-switch

You must enable the global fast-switch function in the global configurative mode before you configure the fast-switch on interface.

command	Function
<b>Ip fast-switch enable</b>	Enable global fast-switch

```

[DEFAULT@Router /config/#ip
.....
(08)fast-switch          Fast switching configuration commands
(09)forward-protocol     Controls forwarding of directed IP broadcasts
.....
Please Input the code of command to be excute(0-20): 8
(00)enable               Enable fast-switch
(01)cache-size           Cache size of fast-switch
(02)timeout              Cache timeout
Please Input the code of command to be excute(0-2): 0
Will you excute it? (Y/N):y

```

## 5. IP section of network protocol configuration

The configuration of protocol IP will be introduced in this chapter. Pay more attention to this chapter because it is the key factor for you to implement your configuration task correctly and rapidly. You will have more understanding about IP addressing and IP service which include the configuration of the significant IP routing.

### 5.1 IP Overview

The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. IP handles addressing, fragmentation, reassembly, and protocol multiplexing. It is the foundation on which all other IP protocols, collectively referred to as the IP Protocol suite, are built. IP is a network-layer protocol that contains addressing and control information that allows data packets to be routed.

The Transmission Control Protocol (TCP) is built upon the IP layer. TCP is a connection-oriented protocol that specifies the format of data and acknowledgments used in the transfer of data. TCP also specifies the procedures that the computers use to ensure that the data arrives correctly. TCP allows multiple applications on a system to communicate concurrently because it handles all demultiplexing of the incoming traffic among the application programs.

The IP address, such as address resolution protocol (ARP) and network address translation (NAT) will be introduced in the “configure IP addressing”. The IP service, such as ICMP, IP statistic and performance parameters and so on will be introduced in the “configure IP service”.

#### 5.1.1 IP Routing Protocol

D-Link router implement various IP routing dynamic protocols. These protocols will be separately introduced in the illustration of protocols of this chapter.

IP routing protocols are divided into two classes: Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP). D-Link router supports RIP, OSPF and BGP. You can separately configure RIP, OSPF and BGP as your requirement. Our router supports to configure various route protocol processes at the same time, which include randomly various OSPF processes (if the memory is enough to be assigned), a BGP process, a RIP process or any amount of BEIGRP process. You can use the command **redistribute** to redistribute routes of other routing protocols into the database of current route process and then connect various routes of multiple protocol process.

To configure the IP dynamic routing protocol, you must set up a corresponding process, connect the respective network interface to certain dynamic routing process and designate the interfaces at which routing process will start. Therefore, you need to view the configuration steps in related configuration command document.

#### 5.1.2 Select a routing protocol

It's a complicated process to select a routing protocol. When you select a routing protocol, you must consider the following factors:

- size and the complexity of the network topology
- whether need to support length-variable network
- network flow
- security
- dependability
- policy
- others

We won't describe this issue any deeper here. However, the user should notice that the routing protocol you select must suit for the condition of your network and meet your requirement.

#### 5.1.3 Interior Gateway Protocols

Interior protocols are used for routing networks that are under a common network administration. All IP interior gateway protocols must be associated with specified network on startup (such as configuring network). Each routing process listens

to updating messages from other routers, and broadcasts its own routing information on the network. The interior routing protocols D-Link supports are as follows:

RIP

OSPF

BEIGRP

## 5.1.4 Exterior Gateway Protocols

Exterior protocols are used to exchange routing information between different autonomous systems. IP exterior gateway protocols normally request configuring the neighbor routers with which to exchange routing information, networks that advertised as directly reachable and the local autonomous system number. D-Link router supports BGP as exterior gateway protocol.

## 5.2 Configure IP Addressing

### 5.2.1 IP Addressing Task List

A basic and necessary task for IP configuration is to assign IP addresses to network interfaces, only with which you can enable an interface and make it have the ability of communicating with other systems by using IP. At one time you should specify the mask IP address.

To configure IP, you should complete tasks in the following sections, the first one is necessary and others are optional. At the end of this chapter, the examples in the "[IP Addressing Example](#)" section illustrate how to set IP addressing.

### 5.2.2 Assign an IP Addresses to a Network Interface

An IP address identifies the destination an IP datagram can reach. Some IP addresses are reserved for special uses and cannot be used for host, subnet, or network addresses. Table 1 lists the range of IP addresses, reserved addresses and available addresses for use.

**Table 1:**

Class	Address or range	Status
A	0.0.0.0	Reserved
	1.0.0.0 to 126.0.0.0	Available
	127.0.0.0	Reserved
B	128.0.0.0 to 191.254.0.0	Available
	191.255.0.0	Reserved
C	192.0.0.0	Reserved
	192.0.1.0 to 223.255.254	Available
	223.255.255.0	Reserved
D	224.0.0.0 to 239.255.255.255	Multicast addresses
E	240.0.0.0 to 255.255.255.254	Reserved
	255.255.255.255	Broadcast address

You can get official description of IP addresses in RFC 1166, "Internet Numbers." And you can contact Internet service provider to achieve an available network address.

An interface can only have one primary IP address. To configure a primary IP address and a network mask to a network interface, you can select **IP** option in the argument prompt of interface configuration and list all arguments:

Command	Task
---------	------

**ip address** *ip-address mask*

Configure master IP address of the interface.

```
(00)access-group      Specify access control for packets
(01)address           IP address
(02)beigrp           Enhanced Interior Gateway Routing Protocol
.....
```

Please Input the code of command to be excute(0-18): 1

Input 1 , select address option, prompt is as below :

```
(00)A.B.C.D          IP address
(01)negotiated       IP address negotiated over PPP or via DHCP
```

Please Input the code of command to be excute(0-1): 0

Input 0 , select A.B.C.D option, prompt is as below :

Please input a IP Address:

Input the primary IP address you want to assign, and the prompt will request inputting mask:

Please input a IP Address:

Input mask, prompt:

```
(00)secondary       Make this IP address a secondary address
(01)<cr>
```

Please Input the code of command to be excute(0-1): 1

Input 1, thus you have complete the configuration of primary IP address.

A mask identifies the network section in an IP address.

---

Note: We only support network masks ordered by network octet and continuously set beginning from the tiptop bit.

---

Other additional and optional tasks will be introduced in the following sections:

[Assign Multiple IP Addresses to a Network Interface](#)

[Enable IP Processing on a Serial Interface](#)

### 5.2.3 Assign Multiple IP Addresses to a Network Interface

Each interface can own multiple IP addresses, including one primary IP address and arbitrary amount of secondary IP addresses. In the following cases you should configure secondary IP address:

There might not be enough host addresses for a particular network segment. For example, a logical subnet has up to 254 valid IP addresses, but in factual application maybe 300 hosts are required to connect in. In this case you can make two logical subnets use a same physical subnet through configuring secondary IP address on your router or your access server.

Some early networks are based on Level2 bridge, but not be split into multiple subnets. Judicious use of secondary address can rebuild a network like such into multiple subnets based on routing. Through secondary IP, a router on a network can acquaint multiple subnets in the same network.

Two subnets of a single network might be separated physically by another network. Here you can make the network addresses to be secondary IP addresses, so that you can connect two subnets in a logical network but divided away physically. <![endif]>

---

Note: If any router on a network segment uses a secondary address, all other routers on that same segment

must also configure secondary addresses of the same network segment.

To assign multiple IP addresses to a network interface, you should select **ip** option in configuring prompt and it will list all arguments:

- (00)access-group            Specify access control for packets
- (01)address                IP address
- (02)beigrp                 Enhanced Interior Gateway Routing Protocol

.....

Please Input the code of command to be excute(0-18): 1

Input 1 , select address option , prompt is as below :

- (00)A.B.C.D                IP address
- (01)negotiated            IP address negotiated over PPP or via DHCP

Please Input the code of command to be excute(0-1): 0

Input 0 , select A.B.C.D option , prompt is as below :

Please input a IP Address:

Input the IP address you want to assign, then prompt is as below:

Please input a IP Address:

Input mask, then prompt is as below:

- (00)secondary            Make this IP address a secondary address
- (01)<cr>

Please Input the code of command to be excute(0-1): 0

Input 0, select secondary option, then you have completed secondary address configuration.

Repeat the steps upwards to implement configuration of multiple IP addresses.

Note : IP routing protocols sometimes treat secondary addresses differently when sending routing updates.

### 5.2.4 Enable IP Processing on a Serial Interface

You might want to enable IP processing on a serial or tunnel interface without assigning an explicit IP address to the interface. Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the interface you specified as the source address of the IP packet. This kind of interface is called unnumbered interface. It also uses the specified interface address in determining which routing processes are sending updates over the unnumbered interface. Restrictions are as follows:

Serial interfaces using HDLC, PPP, LAPB, and Frame Relay encapsulations, as well as tunnel interfaces, can perform IP message processing without assigning IP address. But as it to a serial interface encapsulating frame relay, it must be a point-to-point sub-interface. It is not possible to use this function on interfaces with X.25 or SMDS encapsulations.

You cannot use the **ping** command to determine whether the interface is up, because the interface has no IP address. You can use the Simple Network Management Protocol (SNMP) to monitor interface status remotely. <![endif]>

**Note:** Using an unnumbered serial line between different major networks requires special care. Any routing protocol running on the link should be configured to advertise none information about subnets.

To enable IP processing on an unnumbered serial interface, perform the following command in interface configuration mode:

Command	Task
<b>Ip unnumbered</b> <i>type number</i>	Enable IP process function on a serial or tunnel interface without configuring any IP address.

To enable IP process function on an unnumbered interface, you should select **ip** option in the configuring prompt, and it will list all arguments:

```
(00)access-group      Specify access control for packets
.....
(17)unnumbered       Enable IP processing without an explicit address
(18)unreachables     Enable sending ICMP Unreachable messages
Please Input the code of command to be excute(0-18): 17
Input 17 , select unnumbered option , prompt is as below :
(00)FastEthernet     FastEthernet interface
(01)Ethernet         Ethernet interface
(02)Serial           Serial interface
.....
```

Please Input the code of command to be excute(0-10):

The select the specified type and number.

The specified interface in upward commands must be an other interface holding IP address of the router, but not also an unnumbered interface. And this interface should be also enabled (In showing of command **show interface** the interface is “up”).

An example of how to configure serial interfaces can be found in the "[Serial Interface Configuration Example](#)" section at the end of the chapter.

### 5.2.5 Configure Address Resolution

The IP implementation allows you to control IP address resolution and some other functions. The following sections describe how to configure address resolution:

Establish Address Resolution

Map Host Names to IP Addresses

#### Establish Address Resolution

An IP device can have both a local address, which uniquely identifies the device on its local segment or LAN, and a network address, which identifies the network the device belongs to. The local address is more properly known as a data link address because it is contained in the data link layer part of the packet header and is read by data link devices. The more technically inclined will refer to local addresses as MAC addresses, because the Media Access Control (MAC) sublayer within the data link layer processes addresses for the layer.

To communicate with a device on Ethernet, for example, the router first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called address resolution. The process of determining the IP address from a local data link address is called reverse address resolution.

The router uses two forms of address resolution: Address Resolution Protocol (ARP) and proxy ARP. The ARP and proxy ARP protocols are respectively defined in RFC 826 and RFC 1027.

The Address Resolution Protocol (ARP) is used to associate IP addresses with media or MAC addresses. Taking an IP address as input, ARP determines the associated media address. Once a media or MAC address is determined, the IP address/media address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network.

Perform the following tasks to set address resolution on the router:

Define a Static ARP Cache

Enable Proxy ARP**Define a Static ARP Cache**

ARP and other address resolution protocols provide a dynamic mapping between IP addresses and media addresses. Because most hosts support dynamic address resolution, you generally do not need to specify static ARP cache entries. If you do need to define them, you can do so globally. Doing this task installs a permanent entry in the ARP cache. The router uses this entry to translate 32-bit IP addresses into 48-bit hardware addresses. In addition, you can also specify the router to reply to ARP requests instead of other hosts.

Maybe you do not wish the ARP table live permanently, here you can configure the live time of ARP table. The following two tables list the tasks to provide static mapping between IP addresses and media address.

Command	Task
<b>arp</b> <i>ip-address hardware-address</i>	Globally associate an IP address with a media (hardware) address in the ARP cache.
<b>arp</b> <i>ip-address hardware-address set-alias</i>	Specify that the router respond to ARP requests as if it were the owner of the specified IP address.

In global configure directory, input **arp**, prompt is as below:

```
(00)dynamic      Enable dynamic arp update
(01)A.B.C.D      Host IP address
Please Input the code of command to be excute(0-1): 1
Input 1 , select A.B.C.D option , prompt is as below :
Please input a IP Address:
Input ip-address , prompt is as below :
(00) H:H:H:H:H      48-bit hardware address of ARP entry
Please Input the code of command to be excute(0-0): 0
Input 0 , prompt is as below :
Please input a Hardware Address:
Input hardware-address , prompt is as below :
(00)alias      Respond to ARP requests for the IP address
(01)<cr>
```

Please Input the code of command to be excute(0-1):

Input 1 , then it will map an IP address to a medium address globally in ARP buffer;

Input 0 , select **alias** option , then you specify the router to reply to ARP request of specified IP address with its own MAC address.

Use the following command to configure timeout of the ARP item in ARP buffer:

Command	Task
<b>arp timeout</b> <i>seconds</i>	Set the length of time an ARP cache entry will stay in the cache.

Select 0 option in the prompt, then prompt is as below:

```
(00)timeout      Set ARP cache timeout
Please Input the code of command to be excute(0-0): 0
Input 0 , select timeout option ,
(00)<0-4294967> seconds
```

Please Input the code of command to be excute(0-0): 0  
 Input 0 , prompt is as below :  
 Please input a digital number:Please input a string:  
 Configure timeout value.

To display the ARP timeout value being used on a particular interface, use the **show interfaces** command. Use the **show arp** command to examine the contents of the ARP cache. To remove all nonstatic entries from the ARP cache, use the privileged command **clear arp-cache**.

### Enable Proxy ARP

The router uses proxy ARP, as defined in RFC 1027, to help hosts with no knowledge of routing determine the media addresses of hosts on other networks or subnets. For example, if the router receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to that host through other interfaces, then it generates a proxy ARP reply packet giving its own local data link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host. Proxy ARP is enabled by default.

To enable proxy ARP, select **ip** option in configuring prompt, then select option **proxy-arp**:

Command	Task
<b>ip proxy-arp</b>	Enable ARP on the proxy interface.

### Map a Host Name to an IP Adresse

Each unique IP address can have a host name associated with it. The router maintains a cache of host name-to-address mappings for use by the command **telnet**, **ping**, etc.

To assign host names to addresses, perform the following command in global configuration mode:

Command	Task
<b>ip host <i>name address</i></b>	Statically associate a host name with an IP address.

To specify the map from host name to IP, you should input ip command in global configure directory and it will list all arguments:

```
(00)access-list      Named access-list
.....
(10)host             Add an entry to the IP host name-address table
.....
Please Input the code of command to be excute(0-20): 10
Input 10 ,select host option , prompt is as below :
(00)WORD            Name of host
Please Input the code of command to be excute(0-0): 0
Input 0 ,select WORD option , prompt is as below :
Please input a string :
Input host name, prompt is as below:
(00)A.B.C.D         Host IP address
Please Input the code of command to be excute(0-0): 0
Input 0 ,select A.B.C.D option , input IP address.
```

### Configure a Route Process

As far as you have got before here, you can configure one or more route protocol according to your request. Route protocol provides topology information in Internet. Configuration of IP route protocol, such as BGP, RIP and OSPF will

be introduced in latter documents.

### Configure Broadcasting Message Processing

A broadcast message destined for all hosts on a particular physical network. Network hosts recognize broadcasts by special addresses. Broadcasts are heavily used by some protocols, including several important Internet protocols. Control of broadcast messages is an essential part of the IP network administrator's job. The system supports directed broadcast, i.e. broadcast destined for a special network. Broadcast to all the subnets of a network dose not supported by the system.

Several early IP implementations do not use the current broadcast address standard. Instead, they use the old standard, which calls for all "0" instead of all "1" to indicate broadcast address. Our system can identify and accept messages in both forms.

#### Allow Translation from Directed Broadcast to Physical Broadcast Forward UDP Broadcast Packets and Protocols

### Allow Translation From Directed Broadcast To Physical Broadcast

By default, IP directed broadcast packet will be discarded but not transmitting. The discarded IP directed broadcast packet avoid most of attacking for Router, such as "service denied".

You can enable forwarding of IP broadcasts on an interface where the directed broadcast becomes a physical broadcast. Once the function is enabled, all directed broadcast packets reaching the network the interface residing in will be forwarded to this interface, and then be transmitted as physical broadcast packets.

Perform the following command tasks in interface configuration mode to enable the directed broadcast forwarding:

Command	Task
<b>ip directed-broadcast</b> <i>[access-list-name]</i>	Enable translation from directed broadcast to physical broadcast on an interface.

Select ip option in the prompt, it will list all arguments:

- ```
(00)access-group          Specify access control for packets
(01)address              IP address
(02)beigrp              Enhanced Interior Gateway Routing Protocol
(03)directed-broadcast  Enable forwarding of directed broadcasts
.....
```

Please Input the code of command to be excute(0-19): 3

Input 3 ,select directed-broadcast option ,prompt is as below :

- ```
(00)WORD          - Access-list name
```

Please Input the code of command to be excute(0-0): 0

Input 0 ,select WORD option ,prompt is as below :

Please input Access-list Name:

Input access-list-name.

### Forward UDP Broadcast Packets

Network hosts occasionally use UDP broadcasts to determine address, configuration, and name information. If such a host is on a network segment that does not include a server, UDP broadcasts are normally not forwarded. You can remedy this situation by configuring the interface of your router to forward certain classes of broadcasts to a helper address. You can have more than one helper address per interface.

You can specify a UDP destination port to control which UDP services are forwarded. Current default forward destination port is the UDP packets of NetBIOS name service (port 137).

To enable forwarding and to specify the destination address, perform the following command in interface configuration mode:

Command	Task
<b>ip help-address</b> <i>address</i>	Enable forwarding and specify the destination address for forwarding UDP broadcast packets.

Select ip option in the prompt, it will list all arguments:

```
(00)access-group          Specify access control for packets
.....
(05)helper-address       Specify a destination address for UDP broadcasts
.....
```

Please Input the code of command to be excute(0-19): 5

Input 5 , select helper-address option , prompt is as below :

```
(00) A.B.C.D             IP destination address
```

Please Input the code of command to be excute(0-0): 0

Input 0 , select A.B.C.D option , input IP address.

To specify which protocols will be forwarded, perform the following command in global configuration mode:

Command	Task
<b>ip forward-protocol udp</b> [ <i>port</i> ]	Specify which protocols will be forwarded over which ports.

Input ip command , it will list all arguments:

```
(00)access-group          Specify access control for packets
.....
(09)forward-protocol      Controls forwarding of directed IP broadcasts
.....
```

Please Input the code of command to be excute(0-20): 9

Input 9 , select forward-protocol option , prompt is as below :

```
(00)udp                  Packets to a specific UDP port
```

Please Input the code of command to be excute(0-0): 0

Input 0 , select udp option , prompt is as below:

```
(00)<0-65535>           Port number
```

```
(01)biff                 Biff (mail notification, comsat, 512)
```

```
(02)bootpc              Bootstrap Protocol (BOOTP) client (68)
```

.....

Please Input the code of command to be excute(0-27):

Input protocol to forward.

### Detect and Maintain IP Addressing

Perform the following tasks to detect and maintain the network:

Clear Caches, Tables, and Databases

Display System and Network Statistics

## Clear Caches, Tables, and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database can become necessary when the contents of the particular structure have become or are suspected to be invalid.

The following table lists the command associated with clearing caches, tables, and databases. All are performed in EXEC mode.

Command	Task
<b>clear arp-cache</b>	Clear the IP ARP cache.

Input clear command , it will list all arguments :

```
(00)arp-cache           Clear the entire ARP cache
(01)dialer              Clear dialer statistics
(02)frame-relay-inarp   Clear inverse ARP entries from the map table
.....
```

Please Input the code of command to be excute(0-11): 0

Input 0 , select arp-cache option.

## Display System and Network Statistics

You can display specific router statistics such as the contents of IP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You also can display information about node reachability and discover the routing path that your router's packets are taking through the network.

These commands are summarized in the table that follows. See the "IP Commands" chapter in the Router Products Command Reference for details about the commands listed in these tasks. Perform the following tasks in management directory:

Command	Task
<b>show arp</b>	Display the entries in the ARP table for the router.
<b>show hosts</b>	Display the cached list of host names and IP addresses.
<b>show ip interface</b> [ <i>type number</i> ]	Display the status of interfaces.
<b>show ip route</b> [ <i>protocol</i> ]	Display the current state of the routing table.
<b>ping</b> { <i>host</i>   <i>address</i> }	Test the reachability network node.

Take the first command for an example:

Input show command , prompt is as below:

```
(00)alias           alias for command
(01)arp            ARP table
(02)backup         Bakup status
.....
```

Please Input the code of command to be excute(0-47): 1

Input 1 , select arp option

## IP Addressing Example

Following section provides examples of IP configuration:

### Serial Interfaces Configuration Example

#### Serial Interfaces Configuration Example

In the following example, serial interface (serial 1/0) uses address of ethernet1/1.

```
interface ethernet 1/1
  ip address 202.96.2.3 255.255.255.0
```

```
interface Serial 1/0
  ip unnumbered ethernet 1/1
```

## 5.3 Configuring Network Address Translation (NAT) Task List

### NAT Configuration

Two key problems facing the Internet are depletion of IP address space and scaling in routing. Network Address Translation (NAT) is a feature that allows the IP network of an organization to appear from the outside to use different IP address space than what it is actually using. Thus, NAT allows an organization with non-globally routable addresses to connect to the Internet by translating those addresses into globally routable address space. NAT also allows a more graceful renumbering strategy for organizations that are changing service providers or voluntarily renumbering into classless inter-domain routing (CIDR) blocks. NAT is also described in RFC 1631.

#### 5.3.1 NAT Applications

NAT has several applications. Use it for the following purposes:

You want to connect to the Internet, but not all your hosts have globally unique IP addresses. NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT is configured on the router at the border of a stub domain (referred to as the inside network) and a public network such as the Internet (referred to as the outside network). NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network.

You must change your internal addresses. Instead of changing them, which may be a considerable amount of work, you can translate them by using NAT.

You want to do basic load sharing of TCP traffic. You can map a single global IP address to many local IP addresses by using the TCP load distribution feature.

As a solution to the connectivity problem, NAT is practical only when relatively few hosts in a stub domain communicate outside of the domain at the same time. When this is the case, only a small subset of the IP addresses in the domain must be translated into globally unique IP addresses when outside communication is necessary, and these addresses can be reused when no longer in use.

#### 5.3.2 Benefits of NAT

A significant advantage of NAT is that it can be configured without requiring changes to hosts or routers other than those few routers on which NAT will be configured. As discussed previously, NAT may not be practical if large numbers of hosts in the stub domain communicate outside of the domain. Furthermore, some applications use embedded IP addresses in such a way that it is impractical for a NAT device to translate. These applications may not work transparently or at all through a NAT device. NAT also hides the identity of hosts, which may be an advantage or a disadvantage.

A router configured with NAT will have at least one interface to the inside and one to the outside. In a typical environment, NAT is configured at the exit router between a stub domain and backbone. When a packet is leaving the domain, NAT translates the locally significant source address into a globally unique address. When a packet enters into the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. If the software cannot allocate an address because it has run out of addresses, it will drop the packet.

A router configured with NAT must not advertise the local networks to the outside. However, routing information that NAT receives from the outside can be advertised in the stub domain as usual.

### 5.3.3 NAT Terminology

As mentioned previously, the term *inside* refers to those networks that are owned by an organization and that must be translated. Inside this domain, hosts will have addresses in the one address space, while outside, they will appear to have addresses in another address space when NAT is configured. The first address space is referred to as the local address space and the second is referred to as the global address space.

Similarly, *outside* refers to those networks to which the stub network connects, and which are generally not under the control of the organization. As we will discuss in the following section, a host residing in an outside network can/must be translated into a certain address, and it can be a local or a global address.

Anyhow, NAT uses the following definitions:

**Inside local address**—The IP address that is assigned to a host on the inside network. The address is probably not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.

**Inside global address**—A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world.

**Outside local address**—The IP address of an outside host as it appears to the inside network. Not necessary a legitimate address, it was allocated from address space routable on the inside.

**Outside global address**—The IP address assigned to a host on the outside network by the owner of the host. The address was allocated from globally routable address or network space.

### 5.3.4 NAT Configuration Task List

Before configuring any NAT translation, you must know your inside local addresses and inside global addresses. To configure NAT, perform the optional tasks described in the following sections:

- Translating Inside Source Addresses
- Overloading an Inside Global Address
- Translating Overlapping Addresses
- Providing TCP Load Distribution
- Changing Translation Timeouts
- Monitoring and Maintaining NAT

### 5.3.5 Translating Inside Source Addresses

You can translate your own IP addresses into globally unique IP addresses when communicating outside of your network. You can configure static or dynamic inside source translation as follows:

Static translation establishes a one-to-one mapping between your inside local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

Dynamic translation establishes a mapping between an inside local address and a pool of global addresses.

Figure 1 illustrates a router that is translating a source address inside a network to a source address outside the network

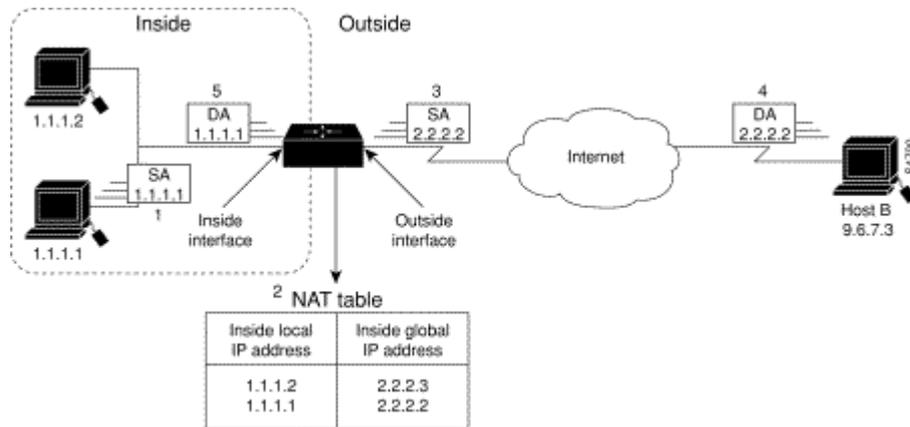


Figure 1 NAT Inside Source Translation

The following process describes inside source address translation, as shown in Figure 1:

1. The user at host 1.1.1.1 opens a connection to host B.
2. The first packet that the router receives from host 1.1.1.1 causes the router to check its NAT table:

If a static translation entry was configured, the router goes to Step 3.

If no translation entry exists, the router determines that Source-Address (SA) 1.1.1.1 must be translated dynamically, selects a legal, global address from the dynamic address pool, and creates a translation entry. This type of entry is called a simple entry.

3. The router replaces the inside local source address of host 1.1.1.1 with the global address of the translation entry and forwards the packet.

4. Host B receives the packet and responds to host 1.1.1.1 by using the inside global IP Destination-Address (DA) 2.2.2.2.

5. When the router receives the packet with the inside global IP address, it performs a NAT table lookup by using the inside global address as a key. It then translates the address to the inside local address of host 1.1.1.1 and forwards the packet to host 1.1.1.1.

Host 1.1.1.1 receives the packet and continues the conversation. The router performs Steps 2 through 5 for each packet.

### 5.3.6 Configuring Static Translation

To configure static inside source address translation, use the following commands in global configuration directory:

Step	Command	Purpose
1	<b>ip nat inside source static</b> <i>local-ip</i> <i>global-ip</i>	Establishes static translation between an inside local address and an inside global address.
2	<b>interface</b> <i>type number</i>	Specifies the inside interface.
3	<b>ip nat inside</b>	Marks the interface as connected to the inside.
4	<b>interface</b> <i>type number</i>	Specifies the outside interface.
5	<b>ip nat outside</b>	Marks the interface as connected to the outside.

Step 1:

Input **ip** command, it will list all arguments:

(00)access-list                  Named access-list

.....  
 (13)nat NAT configuration commands

.....

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

(00)inside Inside address translation  
 (01)log NAT Logging  
 (02)outside Outside address translation

.....

Please Input the code of command to be excute(0-4): **0**

Input 0, select **inside** option , prompt is as below:

(00)source Source address translation  
 (01)destination Destination address translation

Please Input the code of command to be excute(0-1): **0**

Input 0, select **source** option , prompt is as below:

(00)list Specify access list describing local addresses  
 (01)static Specify static local->global mapping

Please Input the code of command to be excute(0-1): **1**

Input 1, select **static** option , prompt is as below:

(00)A.B.C.D Inside local IP address  
 (01)network Subnet translation  
 (02)tcp Transmission Control Protocol  
 (03)udp User Datagram Protocol

Please Input the code of command to be excute(0-3): **0**

Input 0, select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input **local-ip**, prompt is as below:

(00)A.B.C.D Inside Global IP address

Please Input the code of command to be excute(0-0): **0**

Input 0, select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input global-ip.

Step 2 :

Input **interface** command, prompt is as below:

(00)FastEthernet FastEthernet interface  
 (01)Ethernet Ethernet interface  
 (02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify the inside interface type and number.

Step 3 :

Select **18** option in the prompt, it will list all arguments:

(00)access-group Specify access control for packets

.....

(09)nat NAT interface commands

.....

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

(00)inside                    Inside interface for address translation  
 (01)outside                  Outside interface for address translation

Please Input the code of command to be excute(0-1): **0**

Input 0, select **inside** option, it will sign the interface to be connected with inside network.

Step 4 :

Input command **interface** in global configure directory, prompt is as below:

(00)FastEthernet            FastEthernet interface  
 (01)Ethernet                Ethernet interface  
 (02)Serial                   Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify outside interface type and number.

Step 5 :

Select **18** option in the prompt, it will list all arguments:

(00)access-group            Specify access control for packets

.....

(09)nat                       NAT interface commands

.....

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

(00)inside                   Inside interface for address translation  
 (01)outside                  Outside interface for address translation

Please Input the code of command to be excute(0-1): **1**

Input 1, select **outside** option, it will sign the interface to be connected with external network.

The previous steps are the minimum you must configure. You could also configure multiple inside and outside interfaces.

### 5.3.7 Configuring Dynamic Translation

To configure dynamic inside source address translation, use the following commands in global configuration mode:

Step	Command	Purpose
1	<b>ip nat pool</b> <i>name start-ip end-ip netmask</i>	Defines a pool of global addresses to be allocated as needed.
2	<b>ip access-list standard</b> <i>access-list-name</i> config-permit source [source-mask]	Defines a standard access list permitting those addresses that are to be translated
3	<b>ip nat inside source list</b> <i>access-list-name pool name</i>	Establishes dynamic source translation, specifying the access list defined in the prior step.
4	<b>interface</b> <i>type number</i>	Specifies the inside interface.
5	<b>ip nat inside</b>	Marks the interface as connected to the inside.
6	<b>interface</b> <i>type number</i>	Specifies the outside interface.
7	<b>ip nat outside</b>	Marks the interface as connected to the outside.

Step 1.

Input **ip** command , it will list all arguments:

(00)access-list              Named access-list

.....

(13)nat NAT configuration commands

.....

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

(00)inside Inside address translation  
 (01)log NAT Logging  
 (02)outside Outside address translation  
 (03)pool Define pool of addresses  
 (04)translation NAT translation entry configuration

Please Input the code of command to be excute(0-4): **3**

Input 3 , select **pool** option , prompt is as below:

(00)WORD Pool name

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input pool name, prompt is as below:

(00)A.B.C.D Start IP address

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input start ip address , prompt is as below:

(00)A.B.C.D End IP address

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input end ip address , prompt is as below:

(00)A.B.C.D Network mask

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input netmask.

Step 2 :

Input **ip** command , it will list all arguments:

(00)access-list Named access-list  
 (01)as-path BGP as-path access list definition  
 (02)community-list Community attribute list definition

.....

Please Input the code of command to be excute(0-20): **0**

Input 0 , select **access-list** option , prompt is as below:

(00)extended Extended Access List  
 (01)standard Standard Access List

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **standard** option , prompt is as below:

(00)WORD Standard Access-list name

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input access-list-name.

Step 3 :

Input **ip** command , it will list all arguments:

```
(00)access-list      Named access-list
.....
(13)nat              NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

```
(00)inside          Inside address translation
(01)log             NAT Logging
(02)outside         Outside address translation
(03)pool            Define pool of addresses
(04)translation     NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **0**

Input 0 , select **inside** option , prompt is as below:

```
(00)source          Source address translation
(01)destination     Destination address translation
```

Please Input the code of command to be excute(0-1): **0**

Input 0 , select **source** option , prompt is as below:

```
(00)list            Specify access list describing local addresses
(01)static          Specify static local->global mapping
```

Please Input the code of command to be excute(0-1): **0**

Input 0 , select **list** option , prompt is as below:

```
(00)WORD            Access list name for local addresses
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input access-list-name, prompt is as below:

```
(00)interface       Specify interface for global address
(01)pool            Name pool of global addresses
```

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **pool** option , prompt is as below:

```
(00)WORD            Pool name for global addresses
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

```
(00)overload        Overload an address translation
(01)<cr>
```

Please Input the code of command to be excute(0-1): **1**

Input 1 , it will establish the configuration of dynamic source address translation.

Step 4 :

Input **interface** command, prompt is as below:

```
(00)FastEthernet    FastEthernet interface
(01)Ethernet        Ethernet interface
(02)Serial          Serial interface
.....
```

Please Input the code of command to be excute(0-10):

Specify inside interface type and number.

Step 5 :

Select **18** option in the prompt, it will list all arguments:

```
(00)access-group          Specify access control for packets
.....
(09)nat                  NAT interface commands
.....
```

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

```
(00)inside              Inside interface for address translation
(01)outside            Outside interface for address translation
```

Please Input the code of command to be excute(0-1): **0**

Input 0, select **inside** option, it will sign the interface to be connected with inside network.

Step 6 :

Input **interface** command in global configure directory, prompt is as below:

```
(00)FastEthernet        FastEthernet interface
(01)Ethernet            Ethernet interface
(02)Serial              Serial interface
.....
```

Please Input the code of command to be excute(0-10):

Specify outside interface type and number.

Step 7 :

Select **18** option in the prompt, it will list all arguments:

```
(00)access-group          Specify access control for packets
.....
(09)nat                  NAT interface commands
.....
```

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

```
(00)inside              Inside interface for address translation
(01)outside            Outside interface for address translation
```

Please Input the code of command to be excute(0-1): **1**

Input 1, select **outside** option, it will sign the interface to be connected to outside network.

Note: The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access list.) An access list too casual may lead to unpredictable results.

See the "Dynamic Inside Source Translation Example" section at the end of this chapter for an example of dynamic inside source translation.

### 5.3.8 Overloading an Inside Global Address

You can conserve addresses in the inside global address pool by allowing the router to use one global address for many local addresses. When this overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or UDP port numbers) to translate the global address back to the correct local address. When multiple local addresses map to one global address, the TCP or UDP port numbers of each inside host distinguish between the local

addresses.

Figure 2 illustrates NAT operation when one inside global address represents multiple inside local addresses. The TCP port numbers act as differentiators.

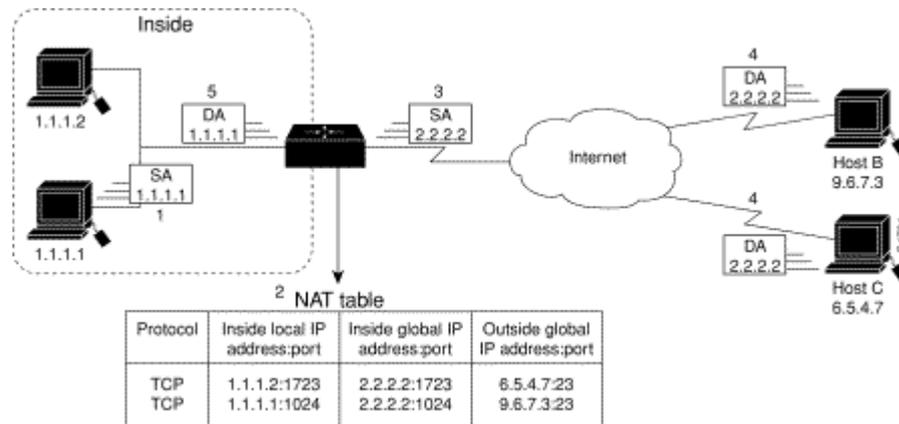


Figure 2 NAT Overloading Inside Global Addresses

The router performs the following process in overloading inside global addresses, as shown in Figure 6. Both host B and host C believe they are communicating with a single host at address 2.2.2.2. They are actually communicating with different hosts; the port number is the differentiator. In fact, many inside hosts could share the inside global IP address by using many port numbers.

1. The user at host 1.1.1.1 opens a connection to host B.

2. The first packet that the router receives from host 1.1.1.1 causes the router to check its NAT table: If no translation entry exists, the router determines that address 1.1.1.1 must be translated, and sets up a translation of inside local address 1.1.1.1 to a legal global address. If overloading is enabled, and another translation is active, the router reuses the global address from that translation and saves enough information to be able to translate back. This type of entry is called an extended entry.

3. The router replaces the inside local source address 1.1.1.1 with the selected global address and forwards the packet.

4. Host B receives the packet and responds to host 1.1.1.1 by using the inside global IP address 2.2.2.2.

5. When the router receives the packet with the inside global IP address, it performs a NAT table lookup, using the protocol, inside global address and port, and outside address and port as a key; translates the address to inside local address 1.1.1.1; and forwards the packet to host 1.1.1.1.

6. Host 1.1.1.1 receives the packet and continues the conversation. The router performs Steps from 2 to 5 for each packet.

To configure overloading of inside global addresses, use the following commands in global configuration mode:

Step	Command	Purpose
1	<b>ip nat pool</b> <i>name start-ip end-ip netmask</i>	Defines a pool of global addresses to be allocated as needed.
2	<b>ip access-list standard</b> <i>access-list-name permit</i> <i>source [source-mask]</i>	Defines a standard access list.
3	<b>ip nat inside source list</b> <i>access-list-name pool name</i>	Establishes dynamic source translation,

	overload	specifying the access list defined in the prior step.
4	<b>interface</b> <i>type number</i>	Specifies the inside interface.
5	<b>ip nat inside</b>	Marks the interface as connected to the inside.
6	<b>interface</b> <i>type number</i>	Specifies the outside interface.
7	<b>ip nat outside</b>	Marks the interface as connected to the outside.

Step 1.

Input **ip** command , it will list all arguments:

```
(00)access-list          Named access-list
.....
(13)nat                  NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

```
(00)inside              Inside address translation
(01)log                 NAT Logging
(02)outside             Outside address translation
(03)pool                Define pool of addresses
(04)translation         NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **3**

Input 3 , select **pool** option , prompt is as below:

```
(00)WORD                Pool name
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input pool name, prompt is as below:

```
(00)A.B.C.D             Start IP address
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input start ip address , prompt is as below:

```
(00)A.B.C.D            End IP address
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input end ip address , prompt is as below:

```
(00)A.B.C.D            Network mask
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input netmask.

Step 2 :

Input **ip** command , it will list all arguments:

```
(00)access-list      Named access-list
(01)as-path          BGP as-path access list definition
(02)community-list  Community attribute list definition
.....
```

Please Input the code of command to be excute(0-20): **0**

Input 0 , select **access-list** option , prompt is as below:

```
(00)extended        Extended Access List
(01)standard        Standard Access List
```

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **standard** option , prompt is as below:

```
(00)WORD            Standard Access-list name
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input access-list-name.

Step 3 :

Input **ip** command , it will list all arguments:

```
(00)access-list      Named access-list
.....
(13)nat              NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

```
(00)inside          Inside address translation
(01)log              NAT Logging
(02)outside          Outside address translation
(03)pool             Define pool of addresses
(04)translation      NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **0**

Input 0 , select **inside** option , prompt is as below:

```
(00)source           Source address translation
(01)destination      Destination address translation
```

Please Input the code of command to be excute(0-1): **0**

Input 0 , select **source** option , prompt is as below:

```
(00)list             Specify access list describing local addresses
(01)static           Specify static local->global mapping
```

Please Input the code of command to be excute(0-1): **0**

Input 0 , select **list** option , prompt is as below:

```
(00)WORD             Access list name for local addresses
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input access-list-name, prompt is as below:

```
(00)interface        Specify interface for global address
(01)pool             Name pool of global addresses
```

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **pool** option , prompt is as below:

(00)WORD Pool name for global addresses

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

(00)overload Overload an address translation

(01)<cr>

Please Input the code of command to be excute(0-1): **0**

Input 0, it will establish configuration of dynamic source address translation.

Step 4 :

Input **interface** command, prompt is as below:

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify inside interface type and number.

Step 5 :

Select **18** option in the prompt, it will list all arguments:

(00)access-group Specify access control for packets

.....

(09)nat NAT interface commands

.....

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

(00)inside Inside interface for address translation

(01)outside Outside interface for address translation

Please Input the code of command to be excute(0-1): **0**

Input 0, select **inside** option, it will sign the interface to be connected with inside network.

Step 6 :

Input **interface** command in global configure directory, prompt is as below:

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify outside interface type and number.

Step 7 :

Select **18** option in the prompt, it will list all arguments:

(00)access-group Specify access control for packets

.....

(09)nat NAT interface commands

.....

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

(00)inside Inside interface for address translation

(01)outside Outside interface for address translation

Please Input the code of command to be excute(0-1): **1**

Input 1, select **outside** option, it will sign the interface to be connected with outside network.

Note: The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access list.) An access list that is too permissive can lead to unpredictable results.

See the "Overloading Inside Global Addresses Example" section at the end of this chapter for an example of overloading inside global addresses.

### 5.3.9 Translating Overlapping Addresses

When an inside local address is identical with an outside address it wants to connect to, address overlapping occurred. Figure 3 shows how NAT translates overlapping networks.

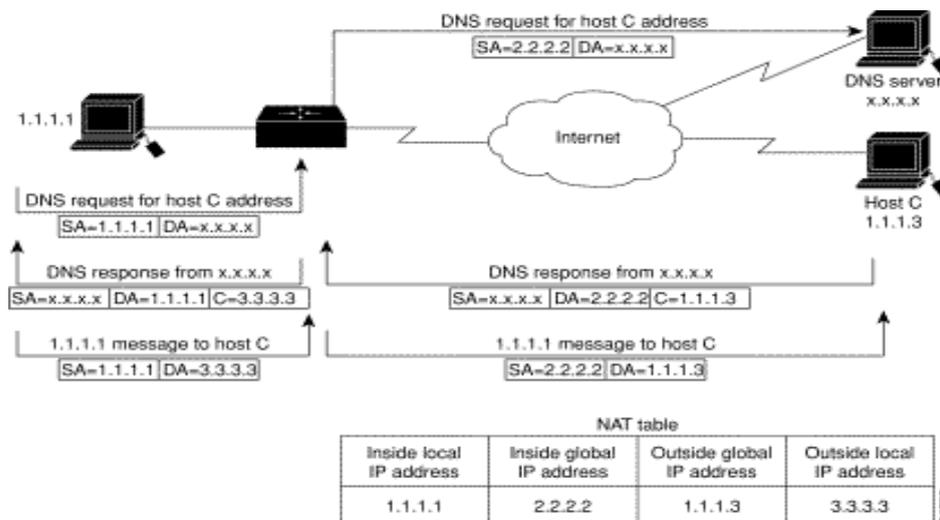


figure 3

The router performs the following process when translating overlapping addresses:

1. The user at host 1.1.1.1 opens a connection to host C by name, requesting a name-to-address lookup from a DNS server.
2. DNS server responds and returns the address 1.1.1.1 of host C. The router intercepts the DNS reply and selects an outside local address from outside local address pool to replace the source address. Here the source address 1.1.1.1 will be replaced by 3.3.3.3.
3. The router sets up translations mapping inside local and global addresses to each other, and outside global and local addresses to each other.
4. The destination address of messages host 1.1.1.1 sends to host C will be an outside local address 3.3.3.3.
5. When router A receives messages destined for outside local addresses, it will translate local address into global address.
6. Host C receives the packet and continues the conversation.

### 5.3.10 Configuring Static Translation

To configure static source address translation, use the following commands in global configure directory:

Step	Command	Purpose
1	<b>ip nat outside source static</b> <i>global-ip</i> <i>local-ip</i>	Establishes static translation between an outside local address and an outside global address.

2	<b>interface</b> <i>type number</i>	Specifies the inside interface.
3	<b>ip nat inside</b>	Marks the interface as connected to the inside.
4	<b>interface</b> <i>type number</i>	Specifies the outside interface.
5	<b>ip nat outside</b>	Marks the interface as connected to the outside.

Step 1 :

Input **ip** command , it will list all arguments:

```
(00)access-list      Named access-list
.....
(13)nat              NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

```
(00)inside          Inside address translation
(01)log             NAT Logging
(02)outside         Outside address translation
(03)pool           Define pool of addresses
(04)translation    NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **2**

Input 2 , select outside option , prompt is as below:

```
(00)source          Source address translation
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **source** option , prompt is as below:

```
(00)list           Specify access list describing global addresses
(01)static         Specify static global->local mapping
```

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **static** option , prompt is as below:

```
(00)A.B.C.D        Outside global IP address
(01)network        Subnet translation
(02)tcp            Transmission Control Protocol
(03)udp            User Datagram Protocol
```

Please Input the code of command to be excute(0-3): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input gobal-ip, prompt is as below:

```
(00)A.B.C.D        Outside local IP address
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input local-ip, it will establish static translation between an outside local address and an outside global address.

Step 2 :

Input **interface** command, prompt is as below:

```
(00)FastEthernet   FastEthernet interface
(01)Ethernet       Ethernet interface
(02)Serial         Serial interface
.....
```

Please Input the code of command to be excute(0-10):

Specify inside interface type and number.

Step 3 :

Select **18** option in the prompt, it will list all arguments:

```
(00)access-group          Specify access control for packets
.....
(09)nat                  NAT interface commands
.....
```

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

```
(00)inside              Inside interface for address translation
(01)outside            Outside interface for address translation
```

Please Input the code of command to be excute(0-1): **0**

Input 0, select inside option, it will sign the interface to be connected with inside network.

Step 4 :

Input **interface** command in global configure directory, prompt is as below:

```
(00)FastEthernet       FastEthernet interface
(01)Ethernet           Ethernet interface
(02)Serial              Serial interface
.....
```

Please Input the code of command to be excute(0-10):

Specify outside interface type and number.

Step 5 :

Select **18** option in the prompt, it will list all arguments:

```
(00)access-group          Specify access control for packets
.....
(09)nat                  NAT interface commands
.....
```

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

```
(00)inside              Inside interface for address translation
(01)outside            Outside interface for address translation
```

Please Input the code of command to be excute(0-1): **1**

Input 1, select outside option, it will sign the interface to be connected to outside network.

### 5.3.11 Configuring Dynamic Translation

To configure dynamic outside source address translation, use the following commands in global configure directory:

Step	Command	Purpose
1	<b>ip nat pool</b> <i>name start-ip end-ip netmask</i>	Defines a pool of local addresses to be allocated as needed.
2	<b>config-ip access-list standard</b> <i>access-list-name</i> <b>config-permit</b> <i>source [source-mask]</i>	Defines a standard access list.
3	<b>config-ip nat outside source list</b> <i>access-list-name pool name</i>	Establishes dynamic outside source translation, specifying the access list defined in the prior step.

4	<b>config-interface</b> <i>type number</i>	Specifies the inside interface.
5	<b>config-ip nat inside</b>	Marks the interface as connected to the inside.
6	<b>config-interface</b> <i>type number</i>	Specifies the outside interface.
7	<b>config-ip nat outside</b>	Marks the interface as connected to the outside.

Step 1.

Input **ip** command , it will list all arguments:

```
(00)access-list          Named access-list
.....
(13)nat                  NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

```
(00)inside              Inside address translation
(01)log                 NAT Logging
(02)outside             Outside address translation
(03)pool                Define pool of addresses
(04)translation        NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **3**

Input 3 , select pool option , prompt is as below:

```
(00)WORD                Pool name
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input pool name, prompt is as below:

```
(00)A.B.C.D            Start IP address
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select A.B.C.D option , prompt is as below:

Please input a IP Address:

Input start ip address , prompt is as below:

```
(00)A.B.C.D End IP address
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input end ip address , prompt is as below:

```
(00)A.B.C.D           Network mask
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select A.B.C.D select , prompt is as below:

Please input a IP Address:

Input netmask.

Step 2 :

Input **ip** command , it will list all arguments:

```
(00)access-list          Named access-list
(01)as-path              BGP as-path access list definition
(02)community-list      Community attribute list definition
```

.....

Please Input the code of command to be excute(0-20): **0**

Input 0 , select **access-list** option , prompt is as below:

(00)extended                    Extended Access List

(01)standard                    Standard Access List

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **standard** option , prompt is as below:

(00)WORD                        Standard Access-list name

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input access-list-name.

Step 3 :

Input **ip** command , it will list all arguments:

(00)access-list                Named access-list

.....

(13)nat                         NAT configuration commands

.....

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

(00)inside                       Inside address translation

(01)log                         NAT Logging

(02)outside                     Outside address translation

(03)pool                        Define pool of addresses

(04)translation                NAT translation entry configuration

Please Input the code of command to be excute(0-4): **2**

Input 2 , select **outside** option , prompt is as below:

(00)source                      Source address translation

(01)destination                Destination address translation

Please Input the code of command to be excute(0-1): **0**

Input 0 , select **source** option , prompt is as below:

(00)list                        Specify access list describing local addresses

(01)static                      Specify static local->global mapping

Please Input the code of command to be excute(0-1): **0**

Input 0 , select **list** option , prompt is as below:

(00)WORD                        Access list name for local addresses

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input access-list-name, prompt is as below:

(00)interface                 Specify interface for global address

(01)pool                        Name pool of global addresses

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **pool** option , prompt is as below:

(00)WORD                        Pool name for global addresses

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

(00)overload Overload an address translation

(01)<cr>

Please Input the code of command to be excute(0-1): **0**

Input 0, it will establish dynamic outside source address translation.

Step 4 :

Input **interface** command, prompt is as below:

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify inside interface type and number.

Step 5 :

Select **18** option in the prompt, it will list all arguments:

(00)access-group Specify access control for packets

.....

(09)nat NAT interface commands

.....

Please Input the code of command to be excute(0-18): **9**

Input 9, select **nat** option, prompt is as below:

(00)inside Inside interface for address translation

(01)outside Outside interface for address translation

Please Input the code of command to be excute(0-1): **0**

Input 0, select inside option, it will sign the interface to be connected to inside network.

Step 6 :

Input **interface** command in global configure directory, prompt is as below:

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify outside type and number.

Step 7 :

Select **18** option in the prompt, it will list all arguments:

(00)access-group Specify access control for packets

.....

(09)nat NAT interface commands

.....

Please Input the code of command to be excute(0-18): **9**

Input 9, select nat option, prompt is as below:

(00)inside Inside interface for address translation

(01)outside Outside interface for address translation

Please Input the code of command to be excute(0-1): **1**

Input 1,select **outside** option, it will sign the interface to be connected to outside network.

Note: The access list must permit only those addresses that are to be translated. (Remember that there

is an implicit "deny all" at the end of each access list.) An access list that is too permissive can lead to unpredictable results.

See the "Translating Overlapping Address Example" section at the end of this chapter for an example of translating an overlapping address.

### 5.3.12 Providing TCP Load Distribution

Another use of NAT is unrelated to Internet addresses. Your organization may have multiple hosts that must communicate with a heavily used host. Using NAT, you can establish a virtual host on the inside network that coordinates load sharing among real hosts. DAs that match an access list are replaced with addresses from a rotary pool. Allocation is done on a round-robin basis, and only when a new connection is opened from the outside to the inside. Non-TCP traffic is passed untranslated (unless other translations are in effect). Figure 4 illustrates this feature.

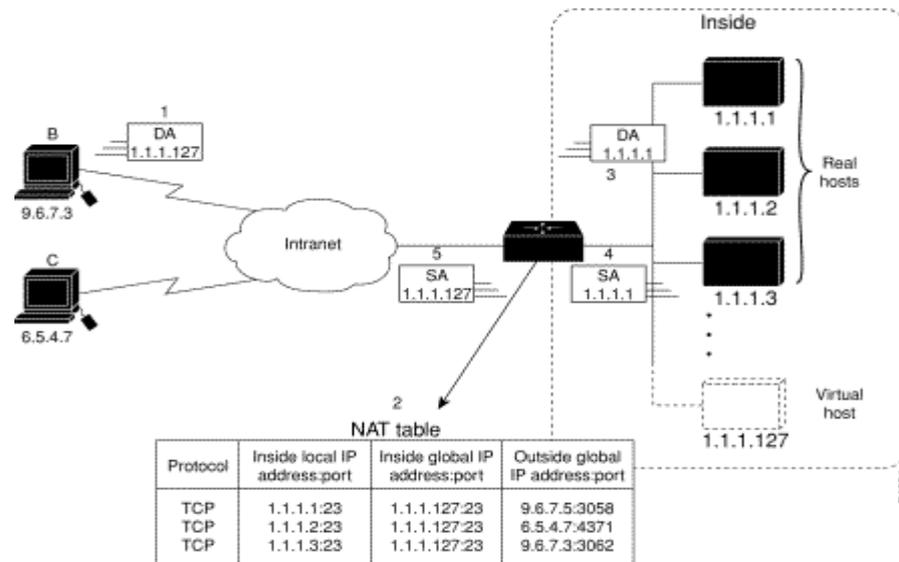


Figure 4 NAT TCP Load Distribution

The router performs the following process when translating rotary addresses:

1. The user on host B (9.6.7.3) opens a connection to the virtual host at 1.1.1.127.
2. The router receives the connection request and creates a new translation, allocating the next real host (1.1.1.1) for the inside local IP address.
3. The router replaces the destination address with the selected real host address and forwards the packet.
4. Host 1.1.1.1 receives the packet and responds.
5. The router receives the packet, performs a NAT table lookup using the inside local address and port number, and the outside address and port number as the key. The router then translates the source address to the address of the virtual host and forwards the packet.

The next connection request will cause the router to allocate 1.1.1.2 for the inside local address. To configure destination address rotary translation, use the following commands beginning in global configuration mode. These commands allow you to map one virtual host to many real hosts. Each new TCP session opened with the virtual host will be translated into a session with a different real host.

Step	Command	Purpose
1	<b>ip nat pool</b> <i>name start-ip end-ip netmask</i>	Defines a pool of addresses containing the addresses of the real hosts.
2	<b>ip access-list standard</b> <i>access-list-name</i>	Defines an access list permitting the

	<b>config-permit</b> <i>source [source-mask]</i>	address of the virtual host.
3	<b>ip nat inside destination list</b> <i>access-list-name</i> <b>pool</b> <i>name</i>	Establishes dynamic inside destination translation, specifying the access list defined in the prior step.
4	<b>interface</b> <i>type number</i>	Specifies the inside interface.
5	<b>ip nat inside</b>	Marks the interface as connected to the inside.
6	<b>interface</b> <i>type number</i>	Specifies the outside interface.
7	<b>ip nat outside</b>	Marks the interface as connected to the outside.

Step 1.

[DEFAULT@router /config/#ip

Key Word:

U(undo) D(default) Q(quit)

```
(00)access-list          Named access-list
.....
(13)nat                  NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13,select **nat** option , prompt is as below:

```
(00)inside              Inside address translation
(01)log                 NAT Logging
(02)outside             Outside address translation
(03)pool                Define pool of addresses
(04)translation         NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **3**

Input 3 , select **pool** option , prompt is as below:

```
(00)WORD                Pool name
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input pool name, prompt is as below:

```
(00)A.B.C.D            Start IP address
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:

Input start ip address , prompt is as below:

```
(00)A.B.C.D End IP address
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:**192.168.1.8**

Input ip address , prompt is as below:

```
(00)A.B.C.D            Network mask
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **A.B.C.D** option , prompt is as below:

Please input a IP Address:**255.255.255.0**

Input netmask.

Step 2 :

Key Word:

U(undo) D(default) Q(quit)

(00)access-list	Named access-list
(01)as-path	BGP as-path access list definition
(02)community-list	Community attribute list definition
.....	

Please Input the code of command to be excute(0-20): **0**

Input 0 , select access-list option , prompt is as below:

(00)extended	Extended Access List
(01)standard	Standard Access List

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **standard** option , prompt is as below:

(00)WORD	Standard Access-list name
----------	---------------------------

Please Input the code of command to be excute(0-0): **0**

Input 0 , select WORD option , prompt is as below:

Please input a string:**name**

Input access list name, **name** only gives a demonstration.

Will you excute it? (Y/N):**y**

Enter into the access list configure mode.

Step 3 :

[DEFAULT@router /config/#]**ip**

Key Word:

U(undo) D(default) Q(quit)

(00)access-list	Named access-list
.....	
(13)nat	NAT configuration commands
.....	

Please Input the code of command to be excute(0-20): **13**

Input 13,select **nat** option , prompt is as below:

(00)inside	Inside address translation
(01)log	NAT Logging
(02)outside	Outside address translation
(03)pool	Define pool of addresses
(04)translation	NAT translation entry configuration

Please Input the code of command to be excute(0-4): **0**

Input 0 , select **inside** option , prompt is as below:

(00)source	Source address translation
(01)destination	Destination address translation

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **destination** option , prompt is as below:

(00)list	Specify access list describing local addresses
(01)static	Specify static local->global mapping

Please Input the code of command to be excute(0-1): **0**

Input 0 , select **list** option , prompt is as below:

(00)WORD                      Access list name for gobal addresses

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

Input access-list-name, prompt is as below:

(00)interface                Specify interface for global address

(01)pool                      Name pool of global addresses

Please Input the code of command to be excute(0-1): **1**

Input 1 , select **pool** option , prompt is as below:

(00)WORD                      Pool name for global addresses

Please Input the code of command to be excute(0-0): **0**

Input 0 , select **WORD** option , prompt is as below:

Please input a string:

(00)overload Overload an address translation

(01)<cr>

Please Input the code of command to be excute(0-1): **1**

Input 1, it will establish dynamic source address translation.

Step 4 :

Input **interface** command, prompt is as below:

(00)FastEthernet              FastEthernet interface

(01)Ethernet                  Ethernet interface

(02)Serial                      Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify inside interface type and number.

Step 5 :

Select option **18** in the prompt, it will list all arguments:

(00)access-group                Specify access control for packets

.....

(09)nat                          NAT interface commands

.....

Please Input the code of command to be excute(0-18): **9**

Input 9, select nat option, prompt is as below:

(00)inside                      Inside interface for address translation

(01)outside                      Outside interface for address translation

Please Input the code of command to be excute(0-1): **0**

Input 0, select **inside** option, it will sign the interface to be connected to inside network.

Step 6 :

Input **interface** command in global configure directory, prompt is as below:

(00)FastEthernet              FastEthernet interface

(01)Ethernet                  Ethernet interface

(02)Serial                      Serial interface

.....

Please Input the code of command to be excute(0-10):

Specify outside interface type and number.

Step 7 :

Select **18** option in the prompt, it will list all arguments:

```
(00)access-group          Specify access control for packets
.....
(09)nat                  NAT interface commands
.....
```

Please Input the code of command to be excute(0-18): **9**

Input 9,select **nat** option, prompt is as below:

```
(00)inside              Inside interface for address translation
(01)outside            Outside interface for address translation
```

Please Input the code of command to be excute(0-1): **1**

Input 1, select **outside** option, it will sign the interface to be connected to outside network.

Note: The access list must permit only those addresses that are to be translated. (Remember that there is an implicit "deny all" at the end of each access list.) An access list that is too permissive can lead to unpredictable results.

See the "TCP Load Distribution Example" section at the end of this chapter for an example of rotary translation.

### 5.3.13 Changing Translation Timeout and Restrict Connection Amount

By default, dynamic address translations time out after some period of nonuse. You can change the default values on timeouts, if necessary. When overloading is not configured, simple translation entries time out after 1 hour. To change this value, use the following command in global configure directory:

Command	Purpose
<b>ip nat translation timeout</b> <i>seconds</i>	Changes the timeout value for dynamic address translations that do not use overloading.

Input **ip** command , it will list all arguments:

```
(00)access-list          Named access-list
.....
(13)nat                 NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13, select nat option , prompt is as below:

```
(00)inside              Inside address translation
(01)log                 NAT Logging
(02)outside            Outside address translation
(03)pool                Define pool of addresses
(04)translation        NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **4**

Input 4 , select **translation** option , prompt is as below:

```
(00)dns-timeout         Specify timeout for NAT DNS flows
.....
(06)timeout             Specify timeout for dynamic NAT translations
.....
```

Please Input the code of command to be excute(0-8): **6**

Input 6 , select **timeout** option , prompt is as below:  
 (00)<0-2147483647> Timeout in seconds  
 (01)never Never timeout  
 Please Input the code of command to be excute(0-1): **0**  
 Input 0 , prompt is as below:  
 Please input a digital number:Please input a string:  
 Input timeout value.

If you have configured overloading, you will have more control over translation entry timeout, because each entry contains more context about the traffic using it. To change timeouts on extended entries, use the following commands in global configuration mode as needed:

Command	Purpose
<b>ip nat translation udp-timeout</b> <i>seconds</i>	Changes the UDP timeout value from 5 minutes.
<b>ip nat translation dns-timeout</b> <i>seconds</i>	Changes the DNS timeout value from 1 minute.
<b>ip nat translation tcp-timeout</b> <i>seconds</i>	Changes the TCP timeout value from 1 hour.
<b>ip nat translation icmp-timeout</b> <i>seconds</i>	Changes the Finish and Reset timeout value from 1 minute.
<b>ip nat translation syn-timeout</b> <i>seconds</i>	Changes the TCP Synchronous (SYN) timeout value from 1 minute.
<b>ip nat translation finrst-timeout</b> <i>seconds</i>	Changes the TCP FIN or RST timeout value from 1 minute.

Take the first command for an example :

Input **ip** command , it will list all arguments:

```
(00)access-list      Named access-list
.....
(13)nat              NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): **13**

Input 13, select **nat** option , prompt is as below:

```
(00)inside          Inside address translation
(01)log             NAT Logging
(02)outside         Outside address translation
(03)pool            Define pool of addresses
(04)translation     NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): **4**

Input 4 , select **translation** option , prompt is as below:

```
(00)dns-timeout     Specify timeout for NAT DNS flows
.....
(07)udp-timeout     Specify timeout for NAT UDP flows
.....
```

Please Input the code of command to be excute(0-8): **7**

Input 7 , select **udp-timeout** option , prompt is as below:

```
(00)<0-2147483647>      Timeout in seconds
(01)never              Never timeout
```

Please Input the code of command to be excute(0-1): **0**

Input 0 , prompt is as below:

Please input a digital number:Please input a string:

Input timeout value.

There are mostly three methods to restrict the amount of NAT connections. You can implement these three methods through executing following commands in global configure mode:

Command	Function
ip nat translation max-entries numbers	Configure the maximum amount of translation items. (Default value is 4000)
ip nat t ranslation max-links A.B.C.D numbers	As to a specified inside IP address, this command will restrict the maximum amount of NAT connection items this IP address can establish.
ip nat translation max-links all numbers	As to all inside IP addresses, this command will restrict the maximum amount of NAT connection items a single IP address can establish.

Take the first command for an example:

Input ip command , it will list all arguments:

```
(00)access-list      Named access-list
.....
(13)nat              NAT configuration commands
.....
```

Please Input the code of command to be excute(0-20): 13

Input 13, select nat option , prompt is as below:

```
(00)inside          Inside address translation
(01)log             NAT Logging
(02)outside         Outside address translation
(03)pool            Define pool of addresses
(04)translation     NAT translation entry configuration
```

Please Input the code of command to be excute(0-4): 4

Input 4 , select translation option , prompt is as below:

```
(00)dns-timeout     Specify timeout for NAT DNS flows
.....
```

```
(03)max-entries     Specify maximum number of NAT entries
.....
```

Please Input the code of command to be excute(0-8): 3

Input 3 , select max-entries option , prompt is as below:

```
(00)<1-2147483647>      Number of entries
```

Please Input the code of command to be excute(0-0): 0

Input 0 , prompt is as below:

Please input a digital number:Please input a string:

Input value of the amount of translation items.

### 5.3.14 Monitoring and Maintaining NAT

By default, dynamic address translations will time out from the NAT translation table at some point. To clear the entries before the timeout, use the following commands in EXEC mode as needed:

Command	Purpose
<b>clear ip nat translation *</b>	Clear all dynamic address translation entries from the NAT translation table.
<b>clear ip nat translation inside</b> <i>local-ip global-ip</i> [ <b>outside</b> <i>local-ip global-ip</i> ]	Clear a simple dynamic translation entry containing an inside translation, or both inside and outside translation.
<b>clear ip nat translation outside</b> <i>local-ip global-ip</i>	Clear a simple dynamic translation entry containing an outside translation.
<b>clear ip nat translation inside</b> <i>local-ip local-port global-ip global-port</i> [ <b>outside</b> <i>local-ip local-port global-ip global-port</i> ]	Clear an extended dynamic translation entry.

Take the first command for an example:

Input **clear** command, it will list all arguments:

- (00)arp-cache                    Clear the entire ARP cache
- (01)dialer                        Clear dialer statistics
- (02)frame-relay-inarp        Clear inverse ARP entries from the map table
- (03)ip                            IP

Please Input the code of command to be excute(0-11): **3**

Input 3 , select **ip** option , prompt is as below:

- (00)beigrp                        Clear BEIGRP
- (01)bgp                            BGP information
- (02)dhcpcd                        DHCP Server information
- (03)fast-switch                Clear FSC
- (04)nat                            Clear NAT
- (05)prefix-list                Prefix list information

Please Input the code of command to be excute(0-5): **4**

Input 4 , select **nat** option , prompt is as below:

- (00)statistics                    Clear translation statistics
- (01)translation                Clear dynamic translation

Please Input the code of command to be excute(0-1): **1**

Input 1 , select translation option , prompt is as below:

- (00)\*                                Delete all dynamic translations
- (01)inside                        Inside addresses
- (02)outside                        Outside addresses
- (03)tcp                            Transmission Control Protocol
- (04)udp                            User Datagram Protocol

Please Input the code of command to be excute(0-4): **0**

Input 0 , it will clear all dynamic address translation items.

To display translation information, use either of the following commands in EXEC mode:

Command	Purpose
<b>show ip nat translations</b> [ <b>verbose</b> ]	Displays active translations.

**show ip nat statistics**

Displays translation statistics.

Take the first command for an example:

Input **show** command, it will list all arguments:

```
(00)alias                alias for command
```

```
.....
```

```
(18)ip                  IP information
```

```
.....
```

Please Input the code of command to be excute(0-45): **18**

Input 18 , select **ip** option , prompt is as below:

```
(00)access-lists       List IP access lists
```

```
.....
```

```
(11)nat                IP NAT information
```

```
.....
```

Please Input the code of command to be excute(0-20): **11**

Input 11 , select **nat** option , prompt is as below:

```
(00)statistics         Translation statistics
```

```
(01)translations       Translation entries
```

```
(02)links              links for specified source address under Overloading rule
```

Please Input the code of command to be excute(0-2): **1**

Input 1 , select **translations** option , prompt is as below:

```
(00)verbose           Show extra information
```

```
(01)<cr>
```

Please Input the code of command to be excute(0-1): **1**

Input 1 , it will show active translation.

### 5.3.15 NAT Configuration Examples

The following sections show NAT configuration examples.

#### Dynamic Inside Source Translation Example

The following example translates all source addresses passing access list 1 (having a source address from 192.168.1.0/24) to an address from the pool named net-208. The pool contains addresses from 171.69.233.208 to 171.69.233.233.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 255.255.255.240
```

```
ip nat inside source list a1 pool net-208
```

```
!
```

```
interface serial1/0
```

```
ip address 171.69.232.182 255.255.255.240
```

```
ip nat outside
```

```
!
```

```
interface ethernet1/1
```

```
ip address 192.168.1.94 255.255.255.0
```

```
ip nat inside
```

```
!
```

```
ip access-list standard a1
```

```
permit 192.168.1.0 255.255.255.0
```

!

### Overloading Inside Global Addresses Example

The following example creates a pool of addresses named net-208. The pool contains addresses from 171.69.233.208 to 171.69.233.233. Access list 1 allows packets having the SA from 192.168.1.0 to 192.168.1.255. If no translation exists, packets matching access list 1 are translated to an address from the pool. The router allows multiple local addresses (192.168.1.0 to 192.168.1.255) to use the same global address. The router retains port numbers to differentiate the connections.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 255.255.255.240
```

```
ip nat inside source list a1 pool net-208 overload
```

!

```
interface serial1/0
```

```
ip address 171.69.232.182 255.255.255.240
```

```
ip nat outside
```

!

```
interface ethernet1/1
```

```
ip address 192.168.1.94 255.255.255.0
```

```
ip nat inside
```

!

```
ip access-list standard a1
```

```
permit 192.168.1.0 255.255.255.0
```

!

### Translating Overlapping Address Example

In the following example, the addresses in the local network are being used legitimately by someone else on the Internet. An extra translation is required to access that external network. Pool net-10 is a pool of outside local IP addresses. The statement, **ip nat outside source list 1 pool net-10**, translates the addresses of hosts from the outside overlapping network to addresses in that pool.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
```

```
ip nat pool net-10 10.0.1.0 10.0.1.255 255.255.255.0
```

```
ip nat inside source list a1 pool net-208
```

```
ip nat outside source list a1 pool net-10
```

!

```
interface serial1/0
```

```
ip address 171.69.232.192 255.255.255.240
```

```
ip nat outside
```

!

```
interface ethernet1/1
```

```
ip address 192.168.1.94 255.255.255.0
```

```
ip nat inside
```

!

```
ip access-list standard a1
```

```
permit 192.168.1.0 255.255.255.0
```

!

### TCP Load Distribution Example

In the following example, the goal is to define a virtual address, connections to which are distributed among a set of real hosts. The pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial interface 0 (the outside interface) whose destination matches the access list are translated to an address from the pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 255.255.255.240
```

```

ip nat inside destination list a2 pool real-hosts
!
interface serial1/0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet1/1
ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
ip access-list standard a2
permit 192.168.15.1 255.255.255.0

```

## 5.4 Configure DHCP Client

DHCP (Dynamic Host Configuration Protocol) provides a part of network configure parameters for hosts in internet. DHCP is introduced in RFC 2131. The most primary function of DHCP in a router is to assign IP addresses to interfaces. DHCP supports three policies of IP address assignment.

1. Automatic allocation: DHCP server assigns a permanent IP automatically to a certain client.
2. Dynamic allocation: DHCP server assigns an IP to a certain client to use for a certain period, or until the client gives up the usufruct of this IP itself.
3. Manual allocation: DHCP server manager specifies an IP manually and transmits it to the client through DHCP.

### 5.4.1 DHCP Applications

DHCP has several applications. When following requests are asked for, it is up to DHCP:

If you want to allocate IP, network segment or some resource (such as corresponding gateway) concerned for an Ethernet interface, you can implement them through DHCP configuration.

If there is an interface on the router connecting with peer device A through PPP, and another interface can access DHCP, then you can get an IP address from DHCP server and assign this IP to device A through IPCP.

### 5.4.2 DHCP Benefits

Current version of the router supports DHCP client. DHCP client is only supported on Ethernet interface, and DHCP message processing is supported on all types of interface. Use of this function can offer the following benefits:

1. Reduce configure time
2. Reduce configure error
3. Centralize the control of IP addresses of some interfaces on a router through DHCP server.

### 5.4.3 DHCP Terms

DHCP per se is based on Server/Client structure, so there are DHCP-Server and DHCP-Client existing in DHCP running.

DHCP-Server: The device used to distribute and take back resource concerned with DHCP.

DHCP-Client: The device achieving information like IP address from DHCP-Server and used it on local system.

As described upward, there is a concept of lease time in the dynamic allocation of DHCP information:

Lease Time: A period of validity of an IP resource timed from its allocating. After this period, the corresponding IP

resource will be taken back by DHCP-Server, and DHCP-Client must send a request again if it wants to keep on using it.

### 5.4.4 DHCP Client Configuration Task List

Before any DHCP is configured, you must ensure that there is at least one DHCP-Server residing in the network the router reachable. Next section will show you how to executing the following optional tasks through DHCP:

1. Obtain an IP for an Ethernet interface.
2. Specify the DHCP-Server address.
3. Configure DHCP parameters.
4. Obtain an IP from DHCP-Server for PPP mutual process
5. Monitor DHCP.

### 5.4.5 Obtain an IP for an Ethernet Interface

Perform the following command on an Ethernet interface to obtain an IP for this interface on the router through DHCP:

Step	Command	Function
1 .	ip address dhcp	Specify using DHCP to configure IP address for the Ethernet interface.

Select 20 option in the prompt , prompt is as below:

- ```
(00)access-group      Specify access control for packets
(01)address           IP address
(02)beigrp            Enhanced Interior Gateway Routing Protocol
.....
```

Please Input the code of command to be excute(0-19): **1**

input 1 , Select address option , prompt is as below:

- ```
(00)A.B.C.D          IP address
(01)dhcp             IP Address negotiated via DHCP
```

Please Input the code of command to be excute(0-1): **1**

input 1 , Selectd hcp option .

### 5.4.6 Specify DHCP-Server

If you have known some DHCP-Server addresses, you can specify these Server addresses on the router to reduce the interaction and time of protocol processing. Perform the following command in global configure directory:

Step	Command	Function
1 .	ip dhcp-server ip-address	Specify the IP address of a DHCP-Server.

input **ip** Command , prompt is as below:

- ```
(00)access-list      Named access-list
.....
(04)dhcp-server      Specify address of DHCP server to use
.....
```

Please Input the code of command to be excute(0-20): **4**

input 4 , Selectd hcp-server option , prompt is as below:

- ```
(00)A.B.C.D          IP address of DHCP Server
```

Please Input the code of command to be excute(0-20): **0**

input 0 , SelectA.B.C.D option , prompt is as below:

Please input a IP Address:

input IP.

When processing “ Obtain an IP for an Ethernet Interface ” , this command is optional.

### 5.4.7 Configure DHCP Parameters

According to your demands, you can adjust the parameters used in DHCP interacting. Perform the following commands in global configure directory:

Step	Command	Function
1 .	ip dhcp client minlease seconds	Specify the minimum lease time allowed.

Step	Command	Function
1 .	ip dhcp client retransmit count	Specify the retransmitting times of a protocol message.

Step	Command	Function
1 .	ip dhcp client select seconds	Specify the interval time of SELECT.

Take the first command for an example. :

input **ip** Command , prompt is as below:

```
(00)access-list          Named access-list
.....
(03)dhcp                Configure DHCP parameters
.....
```

Please Input the code of command to be excute(0-20): **3**

input 3 , Selectdhcp option , prompt is as below:

```
(00)client              Configure DHCP Client parameters
```

Please Input the code of command to be excute(0-0): **0**

input 0 , Selectclient option , prompt is as below:

```
(00)minlease           Minimal acceptable lease time(seconds)
(01)retransmit         Configure packet retransmit count
(02)select             SELECT interval
```

Please Input the code of command to be excute(0-2): **0**

input 0 , Select minlease option , prompt is as below:

```
(00)<60-86400>         seconds (default 60)
```

Please Input the code of command to be excute(0-2): **0**

input 0 , prompt is as below:

Please input a digital number:Please input a string:

input seconds value.

When processing “ Obtain an IP for an Ethernet Interface ” , commands upward are optional.

### 5.4.8 Obtain an IP from DHCP-Server for PPP Interaction

About example of this scheme, please refer to concerned section “ PPP Configure ” .

### 5.4.9 Monitor DHCP

You can examine some information about DHCP-Server (including manual specification) currently found by the router. Perform the following command in management directory:

Step	Command	Function
1 .	show dhcp server	Display information about DHCP Server known by the router.

You can examine some information about IP address currently used by the router. Perform the following command in management directory:

Step	Command	Function
1 .	show dhcp lease	Display information about IP resource used by the router.

input **show** Command , prompt is as below:

```
(00)access-list          Named access-list
```

```
.....
```

```
(11)dhcp                DHCP information
```

```
.....
```

Please Input the code of command to be excute(0-45): **11**

input 11 , Selectdhcp option , prompt is as below:

```
(00)lease                Show DHCP Addresses leased from a server
```

```
(01)server                Show DHCP Servers we know about
```

Please Input the code of command to be excute(0-1):

input 0 , Select lease option , display the IP used by the router as well as concerned information.

input 1 , Select server option , display the information concerned with DHCP server known by the router.

In addition, if you assigned an IP for an Ethernet interface through DHCP, you can also use command “ show interface ” to examine whether the interface has succeeded in obtaining an IP.

### 5.4.10 DHCP Client Configure Example

Following is an example of DHCP Client configure.

#### An Example of Obtaining an IP for an Ethernet Interface

The following example will assign an IP for Ethernet1/1 through DHCP.

```
!
interface Ethernet1/1
 ip address dhcp
```

#### Task List of DHCP Configure

This section will show you how to executing the following optional tasks through DHCP Server:

**Enable DHCP Server Service**

**Disable DHCP Server Service**

**Configure ICMP Inspect Parameters**

**Configure Saving database Parameters**

**Configure DHCP Server Address pool**

**Configure DHCP Server Address pool parameters**

**Monitor DHCP Server**

**Clean DHCP Server Information**

### Enable DHCP Server Service

To enable DHCP Server service and allocate parameters like IP for DHCP Client, please execute the following command in global configure directory (At one time, DHCP Server also supports relay operation. As to some address requests which can't be allocated by itself, we provide ip helper-address port to forward DHCP requests):

Step	Command	Function
1 .	ip dhcpd enable	Enable DHCP Server service.

input **ip** Command , prompt is as below:

```
(00)access-list          Named access-list
.....
(05)dhcpd              Specify server parameter
.....
```

Please Input the code of command to be excute(0-20): **5**

input 5 , Select dhcpd option , prompt is as below:

```
(00)enable             Enable DHCP Service
(01)disable           Disable DHCP Service
(02)pool              Configure DHCP address pools
(03)ping              Specify icmp parameters used by DHCP
(04)write-time        Specify icmp parameters used by DHCP
```

Please Input the code of command to be excute(0-4): **0**

input 0 , Selectenable option .

### Disable DHCP Server service

To disable DHCP Server service and stop allocating parameters like IP for DHCP Client, please execute the following command:

Step	Command	Function
1 .	ip dhcpd disable	Disable DHCP Server service.

input **ip** Command , prompt is as below:

```
(00)access-list          Named access-list
.....
(05)dhcpd              Specify server parameter
.....
```

Please Input the code of command to be excute(0-20): **5**

input 5 , Select dhcpd option , prompt is as below:

```
(00)enable             Enable DHCP Service
(01)disable           Disable DHCP Service
(02)pool              Configure DHCP address pools
(03)ping              Specify icmp parameters used by DHCP
(04)write-time        Specify icmp parameters used by DHCP
```

Please Input the code of command to be excute(0-4): **1**

input 0 , Select disable option .

### Configure ICMP Inspect Parameters

You can adjust the parameters sent by ICMP messages as the server processing address inspecting according to your demands:

To specify the amount of ICMP messages sent out , please execute the following command in global configure directory:

Step	Command	Function
1 .	ip dhcpd ping packets pkgs	Specify the amount of ICMP messages sent out as processing address inspecting.

To configure the timeout waiting for ICMP message, please execute the following command in global configure directory:

Step	Command	Function
1 .	ip dhcpd ping timeout timeout	Specify the timeout for waiting ICMP corresponding.

input **ip** Command , prompt is as below:

```
(00)access-list          Named access-list
.....
(05)dhcpd                Specify server parameter
.....
```

Please Input the code of command to be excute(0-20): **5**

input **5** , Select dhcpd option , prompt is as below:

```
(00)enable              Enable DHCP Serveice
(01)disable            Disable DHCP Service
(02)pool               Configure DHCP address pools
(03)ping               Specify icmp parameters used by DHCP
(04)write-time        Specify icmp parameters used by DHCP
```

Please Input the code of command to be excute(0-4): **3**

input **3** , Selectping option , prompt is as below:

```
(00)packets            Specify number of icmp packets
(01)timeout           Specify icmp timeout
```

Please Input the code of command to be excute(0-1):**0**

Select **0** , specify the amount of sending ICMP messages.

Select **1** , specify the timeout of waiting ICMP corresponding.

Key Word:

Q(quit)

(00)<0-10> Number of ping packets (0 disables ping)

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**2** ( input message amount , 2 is only an example. )

Will you excute it? (Y/N):y

Configure parameters of saving database

To configure the interval of saving the information of address allocation into agent database, please execute the following command in global configure directory:

Step	Command	Function
1 .	ip dhcpd write-time time	Specify the interval of saving the address allocating information into agent database.

input **ip**Command , prompt is as below:

```
(00)access-list          Named access-list
.....
(05)dhcpd                Specify server parameter
```

.....

Please Input the code of command to be excute(0-20): **5**

input 5 , Selectdhcpd option , prompt is as below:

- (00)enable                    Enable DHCP Service
- (01)disable                 Disable DHCP Service
- (02)pool                    Configure DHCP address pools
- (03)ping                    Specify icmp parameters used by DHCP
- (04)write-time              Specify icmp parameters used by DHCP

Please Input the code of command to be excute(0-4): **4**

input 4 , Selectwrite-time option to configure the interval.

Configure DHCP Server address pool

To add DHCP Server address pool , please execute the following command in global configure directory:

Step	Command	Function
1 .	<b>Ip dhcpd pool name</b>	Add DHCP Server address pool and enter into DHCP address pool configuration mode.

input **ip** Command , prompt is as below:

- (00)access-list              Named access-list

.....

- (05)dhcpd                    Specify server parameter

.....

Please Input the code of command to be excute(0-20): **5**

input 5 , Selectdhcpd option , prompt is as below:

- (00)enable                    Enable DHCP Service
- (01)disable                 Disable DHCP Service
- (02)pool                    Configure DHCP address pools
- (03)ping                    Specify icmp parameters used by DHCP
- (04)write-time              Specify icmp parameters used by DHCP

Please Input the code of command to be excute(0-4): **2**

input 2 , Select pool option and add DHCP Server address pool .

Configure parameters of DHCP Server address pool

In configure of DHCP address pool, you can execute the following commands to configure concerned parameters.

You can use the following command to configure the network address used for automatic allocation:

Step	Command	Function
1 .	<b>network ip-addr netsubnet</b>	Configure the network address used for automatic allocation.

You can use this command to configure the address range used for automatic allocation:

Step	Command	Function
1 .	<b>range low-addr high-addr</b>	Configure the address range used for automatic allocation.

You can use this command to configure the default route allocated for client:

Step	Command	Function
------	---------	----------

1 .	<code>default-router ip-addr ...</code>	Configure the default route allocated for client host.
-----	---	--

You can use this command to configure the DNS server address assigned for client:

Step	Command	Function
1 .	<code>dns-server ip-addr ...</code>	Configure the DNS server address assigned for client.

You can use this command to configure the domain name assigned for client:

Step	Command	Function
1 .	<code>domain-name name</code>	Configure the domain name assigned for client.

You can use this command to configure the lease time of address assigned for client:

Step	Command	Function
1 .	<code>lease {days [hours][minutes]   infinite }</code>	Configure the lease time of address assigned for client.

You can use this command to configure the netbios-name-server address assigned for client:

Step	Command	Function
1 .	<code>netbios-name-server ip-addr...</code>	Configure the netbios-name-server address assigned for client.

You can use this command to configure the host address of address pool for manual allocation:

Step	Command	Function
1 .	<code>host ip-addr netmask</code>	Configure the host address of address pool for manual allocation.

You can use this command to configure the hardware address used for matching client:

Step	Command	Function
1 .	<code>hardware-address hardware-address{ type}</code>	Configure the hardware address used for matching client.

You can use this command to configure the client ID used for matching client:

Step	Command	Function
1 .	<code>client-identifier unique-identifier</code>	Configure the client ID used for matching client.

You can use this command to configure the host name used for manual allocating to client:

Step	Command	Function
1 .	<code>client-name name</code>	Configure the host name used for manual allocating to client.

Take the first command for an example. :

In the prompt Select **17** option , prompt is as below:

(00)A.B.C.D            Network number

Please Input the code of command to be excute(0-0): **0**

input 0 , Select A.B.C.D option , prompt is as below:

Please input a IP Address:

input IP.

## Monitor DHCP Server

To examine the information of current address allocating information of the DHCP Server, please execute the following commands in management directory:

Step	Command	Function
1 .	show ip dhcpd binding	Display current address allocating information of the DHCP Server.

To examine current packet statistics of the DHCP Server, please execute the following command in management directory:

Step	Command	Function
1 .	show ip dhcpd statistic	Display current statistics of the DHCP Server.

input show Command ,prompt is as below:

```
(00)alias          alias for command
```

```
.....
```

```
(18)ip            IP information
```

```
.....
```

Please Input the code of command to be excute(0-45): 18

input 18 , Selectip option , prompt is as below:

```
(00)access-lists  List IP access lists
```

```
.....
```

```
(06)dhcpd        DHCP Server information
```

```
.....
```

Please Input the code of command to be excute(0-20): 6

input 6 , Selectdhcpd option , prompt is as below:

```
(00)binding       DHCP address bindings
```

```
(01)statistic     DHCP server statistics
```

Please Input the code of command to be excute(0-1):

Select 0 , display current address allocation of the DHCP Server.

Select 1 ,display current statistics of the DHCP Server.

## Clean DHCP Server information

To clean current address allocating information of the DHCP Server, please execute the following command in management directory:

Step	Command	Function
1 .	clear ip dhcpd binding ip-addr	Clean the specified address allocating information.

To clean current packet statistics of the DHCP Server, please execute the following command in management directory:

Step	Command	Function
1 .	clear ip dhcpd statistic	Clean current packet statistics of the DHCP Server.

input clear Command ,prompt is as below:

```
(00)arp-cache     Clear the entire ARP cache
```

```
(01)dialer        Clear dialer statistics
```

```
(02)frame-relay-inarp  Clear inverse ARP entries from the map table
```

```

(03) ip                IP
    . . . . .
Please Input the code of command to be excute(0-11): 3
input 3 , Select ip option , prompt is as below:
(00)beigrp            Clear BEIGRP
(01)bgp                BGP information
(02)dhcpd             DHCP Server information
    . . . . .
Please Input the code of command to be excute(0-5): 2
input 2 , Select dhcpd option , prompt is as below:
(00)binding           DHCP address bindings
(01)statistic         DHCP server statistics
Please Input the code of command to be excute(0-1):
Select 0 , delete the specified address allocation information.
Select 1 , delete current statistics of the DHCP Server.

```

Example of DHCP Server Configure

Following is an example of DHCP configure.

The following example will configure the timeout of ICMP inspecting to be 200ms, configure an address pool named 1, and enable DHCP Server service.

```

ip dhcpd ping timeout 2
ip dhcpd pool 1
network 192.168.20.0 255.255.255.0
range 192.168.20.211 192.168.20.215
domain-name D-Link315
default-router 192.168.20.1
dns-server 192.168.1.3 61.2.2.10
netbios-name-server 192.168.20.1
lease 1 12 0
!
ip dhcpd enable

```

## 5.5 Configure IP Service Task List

### About IP Service Configuration

This chapter describes how to configure optional IP services. For a complete description of the IP services commands in this chapter, refer to the "IP Services Commands" chapter of the Network Protocols Command Reference.

#### 5.5.1 IP Service Task List

Configure the following IP optional service:

Manage IP Connections

Filter IP Packets

Configure the Hot Standby Router Protocol

Configure Performance Parameters

Configure IP over WANs

Monitor and Maintain the IP Network

Remember that not all the tasks in these sections are required. The tasks you must perform will depend on your network and your needs.

## 5.5.2 Manage IP Connection

The IP suite offers a number of services that control and manage IP connections. Many of these services are provided by the Internet Control Message Protocol (ICMP). ICMP messages are sent by routers to hosts or other routers when a problem is discovered with the Internet header. For detailed information on ICMP, see RFC 792.

To configure IP services, complete the tasks in the following sections:

[Enable ICMP Protocol Unreachable Messages](#)

[Enable ICMP Redirect Messages](#)

[Enable ICMP Mask Reply Messages](#)

[Understand Path MTU Discovery](#)

[Set the IP MTU Packet Size](#)

[Enable IP Source Routing](#)

[Enable IP Fast Switching](#)

[Enable IP Fast Switching in Same Interface](#)

### Send an ICMP Host Unreachable Message

If the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address, it sends an ICMP Host Unreachable message to the source. This feature is enabled by default.

You can enable this service by performing the following command in interface configuration mode:

Command	Task
<code>ip unreachable</code>	Enable the sending of ICMP Protocol Unreachable messages.

Select ip option in the prompt, it will list all arguments:

Key Word:

U(undo) D(default) Q(quit)

.....

(21)rtp Rtp parameters

(22)tcp Tcp parameters

(23)unnumbered Enable IP processing without an explicit address

(24)unreachables Enable sending ICMP Unreachable messages

Please Input the code of command to be execute(0-24):24

Input 24 , Select unreachablees option.

### Sending ICMP Redirect Messages

Routes sometimes can become less than optimal. For example, it is possible for the router to be forced to resend a packet through the same interface on which it was received. If this happens, the router sends an ICMP Redirect message to the packet's originator telling it that it is on a subnet directly connected to the router, and that it must forward the packet to another system on the same subnet. It does so because the originating host presumably could have sent that packet to the next hop without involving the router at all. The Redirect message instructs the sender to remove the router from the route and substitute a specified device representing a more direct path.

This feature is enabled by default. However, when Hot Standby Router Protocol is configured on an interface, ICMP Redirect messages are disabled by default for the interface.

You can enable the sending of ICMP Redirect messages by performing the following task in interface configuration mode:

Command	Task
---------	------

**Ip redirects**

Allow the sending of ICMP Redirect messages.

In the prompt select **ip** option , it will list all arguments.

Key Word:

U(undo) D(default) Q(quit)

.....

- (16)proxy-arp Enable proxy ARP
- (17)redirects Enable sending ICMP Redirect messages
- (18)rip set RIP parameter for this port
- (19)route-cache Enable fast-switching cache for outgoing packets
- (20)rsvp RSVP interface command
- (21)rtp Rtp parameters
- (22)tcp Tcp parameters
- (23)unnumbered Enable IP processing without an explicit address
- (24)unreachables Enable sending ICMP Unreachable messages

Please Input the code of command to be excute(0-24):17

input 17 , Select redirects option .

**Enable ICMP Mask Reply Messages**

Occasionally, the host server must know the subnet mask. To achieve this information, the host server can send ICMP Mask Request messages. These messages are responded to by ICMP Mask Reply messages from router that have the requested information. By default, the router will send ICMP Mask Request messages.

To enable the sending of ICMP Mask Reply messages, use the following command in interface configuration mode:

Command	Purpose
<b>ip mask-reply</b>	Enable the sending of ICMP Mask Reply messages.

In the prompt Select **ip** option , it will list all arguments.

Key Word:

U(undo) D(default) Q(quit)

- (00)access-group Specify access control for packets
- (01)address IP address
- (02)beigrp Enhanced Interior Gateway Routing Protocol
- (03)directed-broadcast Enable forwarding of directed broadcasts
- (04)fast-switch Fast-Switch interface commands
- (05)helper-address Specify a destination address for UDP broadcasts
- (06)igmp IGMP interface command
- (07)irdp ICMP Router Discovery Protocol
- (08)mask-reply Enable sending ICMP Mask Reply messages

.....

Please Input the code of command to be excute(0-18): **8**

input 8 , Select mask-reply option . <![endif]>

**Support Path MTU Discovery**

D-Link routers support the IP Path MTU Discovery mechanism, as defined in RFC 1191. IP Path MTU Discovery allows a host to dynamically discover and cope with differences in the maximum allowable maximum transmission unit (MTU) size of the various links along the path. Sometimes the router finds out that the length of an IP message is larger than

MTU configured on the redirection interface, then the message is needed to be segmented. But if the bit “Don’t Segment” of this IP message is set, the message can only be discarded. Here the router will send out an ICMP message to inform source host about the failing reason and the MTU on redirection interface. Source host will reduce the length of messages to accommodate the least MTU of this route.

If one of the links in route is cut, the message will use another route and maybe its least MTU is different with former route’s. Here the router will inform the source host about MTU of the new route. The least MTU in route should be adopted as much as possible to encapsulate IP message. In that it will avoid segment and send out messages as few as possible. And that can improve the communicating efficiency.

The corresponding host must support IP Route MTU Discovery, thus it can adapt the length of IP messages and avoid the segment in redirection course according the MTU informed by router.

### Set the IP MTU Packet Size

All interfaces have a default MTU packet size. You can adjust the IP MTU size so that if an IP packet exceeds the MTU set for a router's interface, the router will fragment it.

Changing the MTU value can affect the CONFIG-IP MTU value. If the current IP MTU value is the same as the MTU value, and you change the MTU value, the IP MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the mtu interface configuration command. The IP MTU must be less than MTU on current interface configuration. Also, all devices on a physical medium must have the same protocol MTU in order to operate.

To set the IP MTU, perform the following command in interface configuration mode:

Command	Task
<b>ip mtu bytes</b>	Set the IP MTU packet size for an interface.

In the prompt Select **ip** option , it will list all arguments.

```
(00)access-group          Specify access control for packets
```

```
.....
```

```
(08)mtu                  Maximum Transmission Unit
```

```
.....
```

Please Input the code of command to be excute(0-18): **8**

input 8 , Selectmtu option , prompt is as below:

```
(00)<68-1500>          bytes
```

Please Input the code of command to be excute(0-0): **0**

Select0 , prompt is as below:

Please input a string:

```
input the specified IP MTU.    <![endif]>
```

### Enable IP Source Routing

The router examines IP header options on every packet. It supports the IP header options Strict Source Route, Loose Source Route, Record Route, and Time Stamp, which are defined in RFC 791. If the router finds a packet with one of these options enabled, it performs the appropriate action. If it finds a packet with an invalid option, it sends an ICMP Parameter Problem message to the source of the packet and discards the packet. If it finds error in source routing process, it will send and ICMP unreachable (source routing failed) message to the source host.

IP provides a provision allowing the source IP host to specify a route through the IP network. This provision is known as source routing. Source routing is specified as an option in the IP header. If source routing is specified, the router forwards

the packet according to the specified source route. This feature is employed when you want to force a packet to take a certain route through the network. The default is to perform source routing.

You can enable IP source-route header options by performing the following command task in global configuration directory:

Command	Task
<b>ip source-route</b>	Enable the IP source-route

[DEFAULT@router /config/]#**ip**

Key Word:

U(undo) D(default) Q(quit)

(00)access-list Named access-list

(01)as-path BGP as-path access list definition

(02)community-list Community attribute list definition

(03)dhcp Configure DHCP parameters

(04)dhcp-server Specify address of DHCP server to use

(05)dhcpd Specify server parameter

(06)domain-list Domain name to complete unqualified host names

(07)domain-lookup Enable IP Domain Name System hostname translation

(08)fast-switch Fast switching configuration commands

(09)forward-protocol Controls forwarding of directed IP broadcasts

(10)host Add an entry to the IP host name-address table

(11)igmp IGMP global configuration

(12)local Specify local options

(13)mroute Configure static multicast routes

(14)multicast Global IP Multicast Commands

(15)multicast-routing Enable IP multicast forwarding

(16)name-server Specify IP address of domain name server to use

(17)nat NAT configuration commands

(18)pim-dm PIM-DM global commands

(19)prefix-list Prefix list definition

(20)radius RADIUS configuration commands

(21)route static route

(22)rsvp Configure RSVP information

(23)source-route Process packets with source routing header options

(24)tacacs Config TACACS+ information

(25)tcp Global TCP parameters

(26)telnet Specify telnet options

Please Input the code of command to be excute(0-26): **23**

input 23 , Select source-route option .<![endif]>

### Allow IP Fast Exchange

IP Fast Exchange uses routing buffer memory to relay IP message. When relaying the first message to a certain destination, the system will examine routing table and relay the message with the route. And then the route will be kept in the routing buffer memory. Afterwards messages received by this host will be relayed according to the route in buffer against query of routing table. System won't create routing buffer for ICMP messages or broadcasting messages in that generally these messages won't be sent out continuously. If buffer memory is not enough to use, it will be deleted by timeout.

Maybe Fast Exchange is not relevant to use for transmitting from high speed medium to low speed cable (64k or even lower). Because it will quicken the transmitting speed with the result that messages overstock on the low speed interface and more messages are discarded. In that case, IP Fast Exchange should be forbidden on the low speed interface. System will proportion load according to source address / destination address. If there are various network routes existing, Fast Exchange ensures that messages with the same source address / destination address use the same route and that messages with different source address / destination address use various route to transmit respectively, Thus the router proportion the load.

Use commands below in interface configuration status to allow or forbid the Fast Exchange:

Command	Purpose
<b>ip route-cache</b>	Allow Fast Exchange (Relay IP messages with routing buffer).
<b>ip ( undo ) route-cache</b>	Forbid Fast Exchange and system will proportion the load for each message.

In the prompt select **ip** option , it will list all arguments.

U(undo) D(default) Q(quit)

(00)access-group           Specify access control for packets

.....

(13)route-cache           Enable fast-switching cache for outgoing packets

.....

Please Input the code of command to be excute(0-18): **13**

input 13 , Selectroute-cache option , prompt is as below:

(00)same-interface        Enable fast-switching on the same interface

(01)<cr>

Please Input the code of command to be excute(0-1): **1**

input 1 , it will enable fast exchange.

If you select **ip** option in prompt , please first input **D** or **d** , the Select **route-cache** , finally Select **1** , it will disable fast exchange.

### Allow IP Fast Exchange on the Same Interface

User can allow IP Fast Exchange on the same interface, i.e. the interface accepting and transmitting are the same interface. Commonly we suggest that the function don't be opened in that it collides with redirection function in the router. If you have a network of incomplete connection such as frame relay, you can open this function on the frame relay interface. For example, router A, router B and router C constitute a frame relay network, but only the two partners A-B and B-C exist physical link. Communications between A and C must be relayed by B: A-B-C. B gets messages from A through a DLCI on the interface and transmits them to C through another DLCI on the same interface.

Use command below in interface configuration status to allow IP Fast Exchange on the same interface:

Command	Purpose
<b>ip route-cache same-interface</b>	Allow IP messages whose transmitting interface and accepting interface are the same interface.

In the prompt select **ip** option , it will list all arguments.

(00)access-group           Specify access control for packets

.....

(13)route-cache           Enable fast-switching cache for outgoing packets

.....

Please Input the code of command to be excute(0-18): **13**

input 13 , Selectroute-cache option , prompt is as below:

(00)same-interface Enable fast-switching on the same interface

(01)<cr>

Please Input the code of command to be excute(0-1): **0**

input 0 , it will allow fast exchange between messages whose sending interface identical with the receiving interface.

<![endif]>

### Configure Performance Parameters

To tune IP performance, complete any of the tasks in the following sections.

Set the TCP Connection Attempt Time

Set the TCP Window Size

### Configure the Waiting Time of TCP Connection

When router processes TCP connection, if the connection isn't set up after the waiting time of TCP connection, router will consider that the connection fails and return this result to upper applications. User can configure the waiting time of TCP connection and the default value is 75 s. This configuration is foreign to TCP connection and is concerned with TCP connection set up by local router.

Use command below in global configuration status to configure waiting time of TCP connection.

Command	Purpose
<b>ip tcp synwait-time</b> <i>seconds</i>	Set the amount of time that wait to attempt to establish a TCP connection.

[DEFAULT@router /config/#ip

(00)access-list Named access-list

.....

(19)tcp Global TCP parameters

.....

Please Input the code of command to be excute(0-20): **19**

input 19 , Selectsource-route option , prompt is as below:

(00)synwait-time Set time to wait on new TCP connections

(01>window-size TCP window size

Please Input the code of command to be excute(0-1): **0**

input 0 , Selectsynwait-time option , prompt is as below:

(00)<5-300> seconds wait time (default 75 seconds)

Please Input the code of command to be excute(0-1): **0**

Select 0 , and input the wait time. <![endif]>

### Set the TCP Window Size

The default TCP window size is 2000 bytes. To change the default window size, use the following command in global configuration directroy.

Command	Purpose
<b>ip tcp window-size</b> bytes	Set the TCP windows size.

[DEFAULT@router /config/#ip

(00)access-list Named access-list

```

.....
(19)tcp                Global TCP parameters
.....
Please Input the code of command to be excute(0-20): 19
input 19 , Select source-route option  , prompt is as below:
(00)synwait-time      Set time to wait on new TCP connections
(01>window-size       TCP window size
Please Input the code of command to be excute(0-1): 1
input 1 , Select window-size option  , prompt is as below:
(00)<1-65535> bytes    Window size (default 2000)
Please Input the code of command to be excute(0-1): 0
Select0 , and input the window size.  <![endif]>

```

### 5.5.3 Configure IP over WANs

You can configure IP over X.25, Frame Relay, and PPP networks. To do this for X.25, PPP, or Frame Relay, configure the address mappings as described in the appropriate chapters of the Wide-Area Networking Configuration Guide.

#### Monitor and Maintain the IP Network

To monitor and maintain your network, perform the tasks in the following sections:

- Clear Caches, Tables, and Databases
- Clear TCP Connection
- Display System and Network Statistics
- Display Debugging Information

#### Clear Caches, Tables, and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database can become necessary when the contents of the particular structure have become or are suspected to be invalid.

Use the following command to clear:

Command	Purpose
<b>clear tcp statistics</b>	Clear TCP statistics.

```
[DEFAULT@router /enable/]#clear
```

```

(00)arp-cache          Clear the entire ARP cache
.....
(09)tcp                Clear a TCP connection or statistics
.....
Please Input the code of command to be excute(0-11): 9
input 9 , Select tcp option  , prompt is as below:
(00)local              Local host address/port
(01)statistics         TCP protocol statistics
(02)tcb                TCB address
Please Input the code of command to be excute(0-2): 1
input 1 , Select statistics option  , it will clear TCP statistics.

```

Will you excute it? (Y/N):y

#### Clear TCP Connection

Use the following command to shut down a TCP connection.

Command	Purpose
<b>clear tcp</b> { <b>local</b> <i>host-name port</i> <b>remote</b> <i>host-name port</i> / <b>tcb</b> <i>address</i> }	Clear specified TCP connection. (TCB is TCP Control Block.)

[DEFAULT@router /enable/]#clear

(00)arp-cache                    Clear the entire ARP cache

.....

(09)tcp                            Clear a TCP connection or statistics

.....

Please Input the code of command to be excute(0-11): **9**

input 9 , Select tcp option , prompt is as below:

(00)local                        Local host address/port

(01)statistics                  TCP protocol statistics

(02)tcb                          TCB address

Please Input the code of command to be excute(0-2): **0**

input 0 , Select local option , and input the specified connection arguments, it will clear the specified TCP connection.

### Display System and Network Statistics

You can display specific statistics such as the contents of IP routing tables, caches, and databases. The resulting information can be used to determine resource utilization and to solve network problems. Use any of the following commands in privileged EXEC mode. See the "IP Services Commands" chapter for details about the commands listed in these tasks:

Command	Purpose
<b>show ip access-lists</b> <i>name</i>	Display the contents of one or all current access lists.
<b>show ip cache</b> [ <b>prefix mask</b> ] [ <b>type number</b> ]	Display the route cache for fast switching IP message.
<b>show ip sockets</b>	Displays all the IP socket information of router.
<b>show ip traffic</b>	Display IP protocol statistics.
<b>show tcp</b>	Display information of all the TCP connecting status.
<b>show tcp brief</b>	Display the simply information of TCP connection status.
<b>show tcp statistics</b>	Display TCP protocol statistics.
<b>show tcp tcb</b>	Display specified TCP connection status information.

Take the first command for an example. :

[DEFAULT@router /enable/]#show

(00)alias                        alias for command

.....

(18)ip                            IP information

.....

Please Input the code of command to be excute(0-45): **18**

input 18,Select ip , prompt is as below:

(00)access-lists                List IP access lists

(01)as-path-list                Information of AS-Path list

(02)beigrp                        Show BEIGRP information

.....

Please Input the code of command to be excute(0-20): **0**

input 0 , Select access-lists option , prompt is as below:

(00)WORD Access-list name

&lt;cr&gt;

Please Input the code of command to be excute(0-0): **0**

input 0 , SelectWORD option , prompt is as below:

Please input a string:word

input the list string

Will you excute it? (Y/N):y

**Display Debugging Information**When there are some matters in network, you can get the **debug** information with debug commands.

Use commands below in management directory. About the detailed usage of these commands, please refer to the chapter "IP Service Commands".

Command	Purpose
<b>debug arp</b>	Display the interacting information of Address Resolution Protocol (ARP).
<b>debug ip icmp</b>	Display the interacting information of Internet Control Messages Protocol (ICMP).
<b>debug ip raw</b>	Display the received and transmitted IP message information.
<b>debug ip packet</b>	Display the interacting information of Internet Protocol (IP).
<b>debug ip tcp</b>	Display the interacting information of Transfer Control Protocol (TCP).
<b>debug ip udp</b>	Display the interacting information of User Datagram Protocol (UDP).

Take the first command for an example. :

[DEFAULT@router /enable/]#debug

(00)aaa Debug AAA process information

(01)arp IP ARP transactions

(02)backup debug backup information

.....

Please Input the code of command to be excute(0-27): **1**

input 1 , Select arp option .

Will you excute it? (Y/N):y

[DEFAULT@router /enable/]#debug

Key Word:

U(undo) D(default) Q(quit)

.....

(15)ip IP information

(16)job Debug job information

(17)l2tp L2TP information

(18)lapb LAPB information

.....

Please Input the code of command to be excute(0-32): **15 (Select ip)**

Key Word:

```
Q(quit)
(00)beigrp Trace BEIGRP information
(01)bgp trace BGP information
(02)dhcpd DHCP Server activity
(03)icmp ICMP transactions
(04)igmp IGMP protocol activity
(05)igmp host activity
(06)mpacket IP multicast packet operations
(07)mroute-cache IP multicast route cache operations
(08)mrouting IP multicast routing table activity
(09)multicast Multicast services activity
(10)nat NAT debug commands
(11)onlk debug onlk
(12)ospf trace OSPF information
(13)packet IP packet processing
(14)pim-dm Debug PIM-DM
(15)raw Raw IP packet received and sent
(16)rip trace RIP information
(17)rsvp RSVP packet processing
(18)rtp Rtp parameters
(19)tcp TCP information
(20)udp UDP transactions
Please Input the code of command to be excute(0-20):3
input 3 , Select icmp
input 15 , Select raw
input 13 , Select packet
input 19 , Select tcp
input 20 , Select udp
Will you excute it? (Y/N):y
```

## 5.6 Filter IP Packets Task List

### 5.6.1 Filter IP Packets

Packet filtering helps control packet movement through the network. Such control can help limit network traffic and restrict network use by certain users or devices. To permit or deny packets from crossing specified interfaces, D-Link provides access lists. You can use access lists in the following ways:

- To control the transmission of packets on an interface
- To control virtual terminal line access
- To restrict contents of routing updates

This section summarizes how to create IP access lists and how to apply them.

An IP access list is a sequential collection of permission and forbiddance conditions that apply to IP addresses. The D-Link IOS software tests addresses against the conditions in an access list one by one. The first match determines whether the software accepts or rejects the address. Because the software stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the software rejects the address.

The two main tasks involved in using access lists are as follows:

1. Create an access list by specifying an access list number or name and access conditions.
2. Apply the access list to interfaces.

Follwing chapters describe the handling of the two tasks in detail.

## 5.6.2 Create Standard and Extended Access Lists

Creat IP access list by a character string

Note: the standard access list can not have the same name with the extended access list.

To create a standard access list, use one of the following commands in global configuration directory:

Step	Command	Purpose
1	<b>ip access-list standard name</b>	Use the name to define a standard IP access list.
2	<b>deny {source [source-mask]   any}[log] or permit {source [source-mask]   any}[log]</b>	In standard access-list configuration mode, specify one or more conditions allowed or denied. This determines whether the packet is passed or dropped.
3	<b>Quit</b>	Quit the access-list configuration mode.

Step1 :

[DEFAULT@router /config/#ip

```
(00)access-list      Named access-list
(01)as-path          BGP as-path access list definition
(02)community-list  Community attribute list definition
.....
```

Please Input the code of command to be excute(0-20): **0**

input 0 , Select access-list option , prompt is as below:

```
(00)extended          Extended Access List
(01)standard          Standard Access List
```

Please Input the code of command to be excute(0-1): **1**

input 1 , Select standard option , prompt is as below:

```
(00)WORD              Standard Access-list name
```

Please Input the code of command to be excute(0-0): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:

input the list sting.

Step2 :

Key Word:

Q(quit)

```
(00)chinese help message in Chinese
(01)chmem Change memory of system
(02)connect Open a outgoing connection
(03)default restore default configuration
(04)deny Specify packets to reject
(05)disconnect Disconnect an existing outgoing network connection
.....
```

Please Input the code of command to be excute(0-18): **4** (Selectdeny option )

If you Select permit Command, you can specify one or more allowance terms.

In the prompt , prompt is as below:

```
(00)any              Any source host
(01)A.B.C.D          Address to match
```

Please Input the code of command to be excute(0-1): **0**

Key Word:

Q(quit)

```
(00)log logging packet
```

(01)<cr>

Please Input the code of command to be excute(0-1): **0**

Key Word:

Q(quit)

(00)<cr>

Please Input the code of command to be excute(0-0): **0**

Will you excute it? (Y/N):y

To create an extended access list, use one of the following commands in global configuration mode:

Step	Command	Purpose
1	<b>ip access-list extended</b> <i>name</i>	Use the name to define an extended IP access list
2	{ <b>deny</b>   <b>permit</b> } <i>protocol source source-mask destination-mask</i> [ <b>precedence</b> <i>precedence</i> ] [ <b>established</b> ] [ <b>log</b> ]{ <b>deny</b>   <b>permit</b> } <i>protocol any any</i>	In extended access-list configuration mode, specify one condition allowed or denied. This determines whether the packet is passed or dropped. (precedence indicates the priority of ip packet, and <i>precedence</i> indicates Type of Service)
3	<b>Quit</b>	Quit the access-list configuration mode.

Step1 :

input **ip** Command , prompt is as below:

- (00)access-list                   Named access-list
- (01)as-path                      BGP as-path access list definition
- (02)community-list            Community attribute list definition

.....

Please Input the code of command to be excute(0-20): **0**

input **0** , Select access-list option , prompt is as below:

- (00)extended                    Extended Access List
- (01)standard                    Standard Access List

Please Input the code of command to be excute(0-1): **0**

input **0** , Select extended option , prompt is as below:

- (00)WORD                        Extended Access-list name

Please Input the code of command to be excute(0-0): **0**

input **0** , Select WORD option , prompt is as below:

Please input a string:**word** (input extend access list string)

Step2 :

Key Word:

Q(quit)

- (00)chinese help message in Chinese
- (01)chmem Change memory of system
- (02)connect Open a outgoing connection
- (03)default restore default configuration
- (04)deny Specify packets to reject
- (05)disconnect Disconnect an existing outgoing network connection

.....

Please Input the code of command to be excute(0-18):**4** (Select deny option )

If you Select permit Command, you can specify one or more allowance terms.

Key Word:

U(undo) D(default) Q(quit)

(00)<0-255> An IP protocol number

(01)icmp Internet Control Message Protocol

(02)igmp Internet Gateway Message Protocol

(03)ip Internet Protocol

(04)ospf OSPF routing protocol

(05)tcp Transmission Control Protocol

(06)udp User Datagram Protocol

Please Input the code of command to be excute(0-6):**3**( Select corresponding protocol)

Step3 :

Key Word:

Q(quit)

(00)A.B.C.D Address to match

(01)any Any source host

Please Input the code of command to be excute(0-1): **0**

Please input a IP Address:**192.168.1.2**

Key Word:

Q(quit)

(00)A.B.C.D IP subnet mask

Please Input the code of command to be excute(0-0):**0**

Please input a IP Address:**255.255.255.0**

In the prompt input **Q** or **q**, exit from access list configuration.

After you initially create an access list, you place any subsequent additions (possibly entered from the terminal) at the end of the list. In other words, you cannot select ively add access list command lines to a specific access list. However, you can use **permit(undo)** and **deny(undo)** commands to remove entries from a named access list.

Note: When making the standard and extended access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end. Further, with standard access lists, if you omit the mask from an associated IP host address access list specification, 255.255.255.255 is assumed to be the mask.

After creating an access list, you must apply it to a line or interface, as shown in the following section, "Apply the Access List to an Interface ".

### 5.6.3 Apply the Access List to an Interface

After you create an access list, you can apply it to one or more interfaces. Access lists can be applied on either outbound or inbound interfaces.

Use the following command on configuring interface.

Command	Purpose
<b>ip access-group</b> <i>name</i> { <b>in</b>   <b>out</b> }	Apply the access list to interface

In the prompt select **ip** option ,it will list all arguments.

(00)access-group Specify access control for packets

(01)address IP address

(02)beigrp Enhanced Interior Gateway Routing Protocol

.....

Please Input the code of command to be excute(0-18): **0**  
input 0 , Select access-group option , prompt is as below:  
(00)WORD                      Access-list name  
Please Input the code of command to be excute(0-0): **0**  
input 0 , Select WORD option , prompt is as below:  
Please input a string:  
input list string , then prompt is as below:  
(00)in                          Inbound packets  
(01)out                        Outbound packets  
Please Input the code of command to be excute(0-1):  
Select applying the access list to the interface.

The access list can be used in inbound infterface and outbound interface. For inbound access lists, after receiving a packet, the D-Link IOS software checks the source address of the packet against the access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP Host Unreachable message.

For outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. If the access list permits the address, the software transmits the packet. If the access list rejects the address, the software discards the packet and returns an ICMP Host Unreachable message.

If the specified access list dose not existed, the software will transmits all packets.

#### 5.6.4 Extended Access List Examples

In the following example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
 permit tcp any 130.2.0.0 255.255.0.0 gt 1023
 permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface ethernet 1/0
ip access-group aaa in
```

For another example of using an extended access list, suppose you have a network connected to the Internet, and you want any host on an Ethernet to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on the Ethernet except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same two port numbers are used throughout the life of the connection. Mail packets coming in from the Internet will have a destination port of 25. Outbound packets will have the port numbers reversed. The fact that the secure system behind the router always will be accepting mail connections on port 25 is what makes it possible to separately control incoming and outgoing services. The access list can be configured on either the outbound or inbound interface.

In the following example, the Ethernet network is a Class B network with the address 130.20.0.0, and the mail host's address is 130.20.1.2. The keyword established is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicate that the packet belongs to an existing connection.

```
ip access-list aaa
 permit tcp any 130.20.0.0 255.255.0.0 established
 permit tcp any 130.20.1.2 255.255.255.255 eq 25
```

```
interface ethernet 1/0
ip access-group aaa in
```

## 5.7 Configure RIP Task List

### 5.7.1 Configure RIP

This chapter describes how to configure RIP. For a complete description of the RIP commands in this chapter, refer to the "RIP Commands" chapter of the Network Protocols Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

The Routing Information Protocol (RIP) is a relatively old but still commonly used IGP created for use in small, homogeneous networks. It is a classical distance-vector routing protocol in RFC 1058.

RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. Each router sends routing information updates every 30 seconds; this process is termed advertising. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the nonupdating router as being unusable. If there is still no update after 120 seconds, the router removes all routing table entries for the nonupdating router.

The measure, or metric, that RIP uses to rate the value of different routes is the hop count. The hop count is the number of routers that can be traversed in a route. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This small range of metrics makes RIP unsuitable as a routing protocol for large networks.

If the router has a default network path, RIP advertises a route that links the router to the pseudonetwork 0.0.0.0. The network 0.0.0.0 does not exist; RIP treats 0.0.0.0 as a network to implement the default routing feature. Our routers will advertise the default network if a default was learned by RIP, or if the router has a gateway of last resort and RIP is configured with a default metric.

RIP sends updates to the interfaces in the specified networks. If an interface's network is not specified, it will not be advertised in any RIP update.

D-Link router supports plain text and MD5 authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs). For protocol-independent features, see the chapter "IP Routing Protocol-Independent Commands" in this document.

### 5.7.2 RIP Configuration Task List

To configure RIP, complete the tasks in the following sections. You must enable RIP. The remaining tasks are optional.

1. Enable RIP
2. Allow Unicast Updates for RIP
3. Apply Offsets to Routing Metrics
4. Adjust Timers
5. Specify a RIP Version
6. Enable RIP Authentication
7. Disable Route Summarization
8. Disable the Validation of Source IP Addresses
9. Enable or Disable Split Horizon
10. Configure RIP Example
11. Split Horizon Example

### 5.7.3 Enable RIP

To enable RIP, use the following commands, starting in global configuration directory:

Step	Command	Purpose
1	<b>router rip</b>	Enable a RIP routing process, which places you in router configuration mode.
2	network network-number <network-mask>	Associate a network number with a RIP routing process.

Step1 :

input **router** Command , it will list all arguments.

- (00)beigrp Enable BEIGRP (compatible with eigrp)
- (01)bgp Enable Border Gateway Protocol (BGP)
- (02)ospf Enable Open Shortest Path First (OSPF)
- (03)rip Enable Routing Information Protocol(RIP)

Please Input the code of command to be excute(0-3): **3** (Select rip option )

Will you excute it? (Y/N):y

Step2 :

Key Word:

Q(quit)

(00)auto-summary Config automatic network number summarization

(01)chinese help message in Chinese

(02)chmem Change memory of system

(03)connect Open a outgoing connection

(04)default restore default configuration

(05)default-information Control distribution of default information

(06)default-metric Set metric of redistributed routes

(07)disconnect Disconnect an existing outgoing network connection

(08)distance Set administrative distance

(09)english help message in English

(10)exit exit / quit

(11)filter Set route filter to the networks in routing updates

(12)help Description of the interactive help system

(13)history look up history

(14)input-queue Specify input queue depth

(15)interface interface configuration

(16)neighbor Specify a neighbor router

(17)network enable RIP on an IP network

(18)no negate configuration

(19)offset Add offset for RIP routes

(21)redistribute Redistribute information from another protocol

(22)resume Resume an active outgoing network connection

(23)router routing protocol configuration

(24)show show configuration and status

(25)telnet Open a telnet connection

(26)timers Adjust routing timers

(27)validate-update-source whether to validate-update-source

(28)version Set routing protocol version

(29)where display all outgoing telnet connection

Please Input the code of command to be excute(0-29): **17** (Select network option )

Key Word:

U(undo) D(default) Q(quit)

(00)A.B.C.D Network number

Please Input the code of command to be excute(0-0):**0**

(00)A.B.C.D Network number

Please Input the code of command to be excute(0-0): **0**

input 0 , Select A.B.C.D option , prompt is as below:

Please input a IP Address : **192.168.1.8** ( input network number )

(00)A.B.C.D Network mask

(01)<cr>

Please Input the code of command to be excute(0-1): **0**

Please input a IP Address:**255.255.255.0** ( input mask )

#### 5.7.4 Allow Unicast Updates for RIP

Because RIP is normally a broadcast protocol, in order for RIP routing updates to reach nonbroadcast networks, you must configure the D-Link IOS software to permit this exchange of routing information. To do so, use the following command in router configuration directory:

Command	Purpose
<b>neighbor</b> <i>ip-address</i>	Define a neighboring router with which to exchange routing information.

Key Word:

Q(quit)

(00)auto-summary Config automatic network number summarization

(01)chinese help message in Chinese

(02)chmem Change memory of system

(03)connect Open a outgoing connection

(04)default restore default configuration

(05)default-information Control distribution of default information

(06)default-metric Set metric of redistributed routes

(07)disconnect Disconnect an existing outgoing network connect ion

(08)distance Set administrative distance

(09)english help message in English

(10)exit exit / quit

(11)filter Set route filter to the networks in routing upd ates

(12)help Description of the interactive help system

(13)history look up history

(14)input-queue Specify input queue depth

(15)interface interface configuration

(16)neighbor Specify a neighbor router

.....

Please Input the code of command to be excute(0-29): **16** (Select neighbor option )

(00)A.B.C.D gateway IP address

Please Input the code of command to be excute(0-0): **0**

Please input a IP Address:**192.168.1.8**(input IP )

In addition, to control the set of interfaces with which you want to exchange routing updates, you can disable the sending of routing updates on specified interfaces by configuring the **ip rip passive** command. See the discussion on filtering in

the "Filter Routing Information" section in the "Configuring IP Routing Protocol-Independent Commands" chapter.

### 5.7.5 Apply Offsets to Routing Metrics

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. This is done to provide a local mechanism for increasing the value of routing metrics. Optionally, you can limit the offset list with either an access list or an interface. To increase the value of routing metrics, use the following command in router configuration mode:

Command	Purpose
<b>offset-list</b> { [ <i>interface-type number</i> ]* } { <b>in out</b> } <i>access-list-name offset</i>	Apply an offset to routing metrics.

Key Word:

Q(quit)

(15)interface interface configuration

(16)neighbor Specify a neighbor router

(17)network enable RIP on an IP network

(18)no negate configuration

(19)offset Add offset for RIP routes

(21)redistribute Redistribute information from another protocol

(22)resume Resume an active outgoing network connection

Please Input the code of command to be excute(0-29): **19** (Select offset option )

(00)\* All interface

(01)interface-name

Please Input the code of command to be excute(0-1): **1**(Select interface-name)

Please input a interface name:

input interface type and number , prompt is as below:

(00)in adding offset for incoming routing updates

(01)out adding offset for outgoing routing updates

Please Input the code of command to be excute(0-1):

input **0** , Select inbound , input **1** , Select outbound , then prompt is as below:

(00)WORD Name of IP access list

Please Input the code of command to be excute(0-0): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:**word**( input string )

(00)<0-16> Offset

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:Please input a string:**2**(input offset)

### 5.7.6 Adjust Timers

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs.

It also is possible to tune the IP routing support in the software to enable faster convergence of the various IP routing algorithms, and, hence, quicker fallback to redundant routers. The total effect is to minimize disruptions to end users of the network in situations where quick recovery is essential. To adjust the timers, use the following commands in router

configuration mode:

Command	Purpose
<b>timers holddown</b> <i>value</i>	How long (Unit: second) to delete a route from route table.
<b>timers expire</b> <i>value</i>	How long (Unit: second) the route to be advertised as invalidation.
<b>timers update</b> <i>value</i>	Transmit the frequency of route update (interval of transmit update, unit: second)

Take the first command for an example. :

In the prompt select **timers** option , prompt is as below:

```
(00)holddown          holddown interval
(01)expire            expire interval
(02)update            interval of routing updates
```

Please Input the code of command to be excute(0-2): **0**

input 0 , Select holddown option , prompt is as below:

```
(00)<1-4294967295>    interval(in second)
```

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:Please input a string:**5**(input time value)

### 5.7.7 Specify a RIP Version

D-Link router RIP version 2 supports authentication, key management, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

By default, the software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the software to receive and send only Version 1 packets. Alternatively, you can configure the software to receive and send only Version 2 packets. To do so, use the following command in router configuration mode:

Command	Purpose
<b>version</b> {1   2}	Configure the router to receive and send only RIP Version 1 or only RIP Version 2 packets.

In the prompt select **version** option , prompt is as below:

```
(00)1                only version 1 RIP
(01)2                only version 2 RIP
```

Please Input the code of command to be excute(0-1):

Select RIP version .

The preceding task controls the default behavior of RIP. You can override that behavior by configuring a particular interface to behave differently. To control which RIP version an interface sends, use one of the following commands in interface configuration mode:

Command	Purpose
<b>ip rip send version 1</b>	Configure an interface to send only RIP Version 1 packets.
<b>ip rip send version 2</b>	Configure an interface to send only RIP Version 2 packets.
<b>ip rip send version compatibility</b>	Broadcast RIP-2 update message

In the prompt select **ip** option , prompt is as below:

```
(00)access-group          Specify access control for packets
.....
(12)rip                  set RIP parameter for this port
.....
```

Please Input the code of command to be excute(0-18): **12**(Select rip option )

```
(00)authentication      Enable authentication mode
.....
(05)send                Advertisement transmission in the interface
.....
```

Please Input the code of command to be excute(0-6): **5**(Select send option )

```
(00)version             send version control
```

Please Input the code of command to be excute(0-0): **0**

input 0 , Select version option , prompt is as below:

```
(00)1 Send version 1 update
(01)2 Send version 2 update
(02)compatibility version 2 update are broadcast
```

Please Input the code of command to be excute(0-2):

```
input 0 , then interface will only send RIP-1 packets.
input 1 , then interface will only send RIP-2 packets.
input 2 , then interface will broadcast RIP-2 updating messages.
```

Similarly, to control how packets received from an interface are processed, use one of the following commands in interface configuration mode:

Command	Purpose
<b>ip rip receive version 1</b>	Configure an interface to accept only RIP Version 1 packets.
<b>ip rip receive version 2</b>	Configure an interface to accept only RIP Version 2 packets.
<b>ip rip receive version 1 2</b>	Configure an interface to accept either RIP Version 1 or 2 packets.

### 5.7.8 Enable RIP Authentication

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface.

We support two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP Version 2 packet is plain text authentication.

Note: Do not use plaintext authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP Version 2 packet. Use plain text authentication when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

To configure RIP plain text authentication, use the following commands in interface configuration mode:

Step	Command	Purpose
1	<b>ip rip authentication simple</b>	Enable RIP authentication

2	<b>ip rip password</b> [string]	Configure the interface to use plain text authentication
---	---------------------------------	--

Step1 :

In the prompt select **ip** option , prompt is as below:

```
(00)access-group      Specify access control for packets
.....
(12)rip              set RIP parameter for this port
.....
```

Please Input the code of command to be excute(0-18): **12**(Select rip option )

```
(00)authentication   Enable authentication mode
(01)message-digest-key  Config md5 authentication key and key-id
(02)passive          Only receive Update in the interface
.....
```

Please Input the code of command to be excute(0-6): **0**

input 0 , Select authentication , prompt is as below:

```
(00)message-digest    Use message-digest authentication
(01)simple            Use simple authentication
```

Please Input the code of command to be excute(0-1): **1**

input 1 , Select simple option , enable authentication.

Step2 :

In the prompt select **ip** option , prompt is as below:

```
(00)access-group      Specify access control for packets
.....
(12)rip              set RIP parameter for this port
.....
```

Please Input the code of command to be excute(0-18): **12**

input 12 , Select rip option , prompt is as below:

```
(00)authentication   Enable authentication mode
(01)message-digest-key  Config md5 authentication key and key-id
(02)passive          Only receive Update in the interface
(03)password         Config simple authentication password
.....
```

Please Input the code of command to be excute(0-6): **3**

input 3 , Select password , prompt is as below:

```
(00)WORD            Authentication key(16 char)
```

Please Input the code of command to be excute(0-1): **0**

input 1 , Select WORD option , prompt is as below:

Please input a string:

input string , specify the interface use plaintext authentication.

To configure RIP MD5 authentication, use the following commands in interface configuration mode:

Step	Command	Purpose
1	<b>ip rip authentication message-digest</b>	Enable RIP authentication
2	<b>ip rip message-digest-key</b> [key-ID] <b>md5</b> [key]	Configure the interface to use MD5 digest authentication

### 5.7.9 Disable Route Summarization

RIP Version 2 supports automatic route summarization by default. The software summarizes subprefixes to the classful network boundary when crossing classful network boundaries.

If you have a disconnected subnet, you should disable automatic route summarization to advertise the subnet. When route summarization is disabled, the software transmits subnet and host routing information across classful network boundaries. To disable automatic summarization, use the following command in router configuration mode:

Command	Purpose
<b>auto-summary (undo)</b>	Disable automatic summarization

### 5.7.10 Disable the Validation of Source IP Addresses

By default, the software validates the source IP address of incoming RIP routing updates. If that source address is not valid, the software discards the routing update.

You might want to disable this feature if you have a router that is "off network" and you want to receive its updates. However, disabling this feature is not recommended under normal circumstances. To disable the default function that validates the source IP addresses of incoming routing updates, use the following command in router configuration mode:

Command	Purpose
<b>validate-update-source (undo)</b>	Disable the validation of the source IP address of incoming RIP routing updates.

### 5.7.11 Enable or Disable Split Horizon

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and SMDS), situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon.

If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon, use one of the following commands in interface configuration mode:

Command	Purpose
<b>ip rip split-horizon</b>	Enable split horizon
<b>ip (undo) rip split-horizon</b>	Disable split horizon

In the prompt Select **ip** option , prompt is as below:

```
U(undo) D(default) Q(quit)
(00)access-group          Specify access control for packets
.....
```

(12)rip                            set RIP parameter for this port

.....

Please Input the code of command to be excute(0-18): **12**

input 12 , Select rip option , prompt is as below:

(00)authentication                Enable authentication mode  
 (01)message-digest-key            Config md5 authentication key and key-id  
 (02)passive                        Only receive Update in the interface

.....

(06)split-horizon                set split horizon for this port

Please Input the code of command to be excute(0-6): **6**

input 0 , Select split-horizon option ,then enable split-horizon.

If you In the prompt Select **ip** option ,please first Select **U** or **u** ,then Select rip option and split-horizon option ,then it will disable split-horizon.

As it to point-to-point interfaces, split horizon is enabled by default; As it to point-to-multipoint, split horizon is disabled by default.

See the "Split Horizon Examples" section at the end of this chapter for examples of using split horizon.

Note: In general, changing the state of the default is not recommended unless you are certain that your application requires making a change in order to advertise routes properly. Remember: If split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you must disable split horizon for all routers in any relevant multicast groups on that network.

### 5.7.12 Monitor and Maintain RIP

In Monitoring and maintaining RIP, you can some network statistics, such as: RIP parameters, network usage, real time tracing of network communicating and so on. Such information will assist you to examine the network usage so that you can resolve network problems. You can also acquaint the reachability of network nodes.

Use these commands in management directory to show several statistics:

input show Command , prompt is as below:

(00)alias        alias for command

.....

(18)ip        IP information

.....

Please Input the code of command to be excute(0-45): **18**

input 18 , select ip option , prompt is as below:

(00)access-lists        List IP access lists

.....

(14)rip        Routing Information Protocol(RIP)

.....

Please Input the code of command to be excute(0-20): **14**

input 14 , Select rip option , prompt is as below:

(00)database        rip route  
 (01)protocol        rip protocol  
 (02)<cr>        show current status of RIP protocol

Please Input the code of command to be excute(0-2):

input **0** , display all RIP routes ;

input **1** , display RIP concerned information ;  
input **2** , display RIP current status.

You can also use following commands in management directory to trace the routing information:

Command	Purpose
debug ip rip database	Trace the routing information, such as RIP route adding in routing table, deleting route from routing table, route changing and so on.
debug ip rip protocol	Trace RIP messages.

### 5.7.13 RIP Configuration Examples

This section contains RIP split horizon configuration examples:

RIP basic configuration

Two routers of 17 series, configuring as below:

Router A

```
interface ethernet 1/1
 ip address 192.168.20.81 255.255.255.0
!
interface loopback 0
 ip address 10.1.1.1 255.0.0.0
!
router rip
 network 192.168.20.0
 network 10.0.0.0
!
```

Router B

```
interface ethernet 1/1
 ip address 192.168.20.82 255.255.255.0
interface loopback 0
 ip address 20.1.1.1 255.0.0.0
!
router rip
 network 192.168.20.0
 network 20.0.0.0
!
```

## 5.8 Configure BEIGRP Dynamic Route Protocol

This section will describes the configuring process of BEIGRP dynamic route protocol.

### 5.8.1 Brief Introduction of BEIGRP Route Protocol

BEIGRP uses the same distance vector algorithm:

- Router will make the routing policy only depending on the information supported by directly connected neighbor;
- Router will only provide its routing information to directly connecting neighbors.

But there are some primary differences between BEIGRP and metric, which make BEIGRP has more advantages:

- BEIGRP will keep all routes in topology-list sent from all neighbors but not only optimal routes got so far;
- BEIGRP is able to process query when there's no destination address or replacing route, so the convergence rate of BEIGRP can match one in optimal link status protocol.

DUAL (Diffused Update Algorithm) is the key to the advantages of BEIGRP over other traditional metric routing protocols. It always works actively so that BEIGRP is able to query to neighbors when there's no destination address or replacing route. Because summary is active but not passive (passively wait for route overtime), so the summary speed of BEIGRP is high.

BEIGRP is a special transfer protocol designed for the request of EIGRP and is built on IP. It meets BEIGRP demands below:

- Dynamically find out the appearance of new neighbors and disappearance of old neighbors through Hello messages.
- So the data and the transmission are both reliable
- Transfer protocol allows unicast and multicast.
- Transfer protocol per se can accommodate to the variety of network terms and the variety of neighbor response.
- BEIGRP can confine its bandwidth-percent according to demand.

### 5.8.2 BEIGRP Configuration Task List

To configure BEIGRP, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional:

- Enable BEIGRP
- Configure the Percentage of Link Bandwidth Used
- Adjust the BEIGRP Calculating Coefficient of Metrics
- Apply offset-list to Adjust Routing Metrics
- Disable Route Automatic Summarization
- Customize Route Summarization
- Configure BEIGRP Protocol-Independent Parameters
- Monitor and Maintain BEIGRP

### 5.8.3 Enable BEIGRP

To create a BEIGRP routing process, perform the following commands in order:

Step	Command	Purpose
1	<b>router beigrp</b> <i>as-number</i>	Enable an BEIGRP routing process in global configuration mode.
2	<b>network</b> <i>network-number</i> <i>network-mask</i>	Associate networks with an BEIGRP routing process in router configuration mode.

```
[DEFAULT@Router /config/]#router
```

Key Word:

U(undo) D(default) Q(quit)

(00)beigrp Enable BEIGRP (compatible with eigrp)

(01)bgp Enable Border Gateway Protocol (BGP)

(02)ospf Enable Open Shortest Path First (OSPF)

(03)rip Enable Routing Information Protocol(RIP)

Please Input the code of command to be execute(0-3): 0

input 0 , Select beigrp option :

Key Word:

Q(quit)

(00)<1-65535> BEIGRP AS Number

Please Input the code of command to be excute(0-0): 0

input 0 , Select <1-65535> option :

Please input a digital number:Please input a string:23

Note: Here input BEIGRP program amount , 23 is only an example..

Will you excute it? (Y/N):y

Key Word:

Q(quit)

(00)auto-summary Config automatic network number summarization

(01)beigrp config beigrp

(02)chinese help message in Chinese

(03)chmem Change memory of system

(04)default restore default configuration

(05)default-metric Set metric of redistributed routes

(06)distance Set administrative distance

(07)english help message in English

(08)exit exit / quit

(09)filter Set route filter to the networks in routing updates

(10)help Description of the interactive help system

(11)history look up history

(12)interface interface configuration

(13)metric Modify BEIGRP routing metrics and parameters

(14)network Enable BEIGRP on an IP network

(15)no negate configuration

(16)offset Add offset for BEIGRP routes

(18)redistribute Redistribute information from another protocol

(19)router routing protocol configuration

(20)show show configuration and status

(21)timers Adjust routing timers

Please Input the code of command to be excute(0-21): 14

Select network

Key Word:

U(undo) D(default) Q(quit)

(00)A.B.C.D Network number

Please Input the code of command to be excute(0-0): 0

input 0 , Select A.B.C.D option :

Please input a IP Address:192.168.19.80

Note:here input IP , 192.168.19.80 is only an example..

Key Word:

Q(quit)

(00)A.B.C.D Network mask

(01)<cr> <cr>

Please Input the code of command to be excute(0-1):0

input 0 , Select A.B.C.D option

Please input a IP Address:255.255.0.0

Note:here input mask address , 255.255.0.0 is only an example..

Will you excute it? (Y/N):y

After the upper configurations, BEIGRP will start to function on all interfaces belonging to this segment. It will find out new neighbors through Hello and process initial routing exchange through Update.

#### 5.8.4 Configure the Percentage of Link Bandwidth Used

By default, BEIGRP packets consume a maximum of 50 percent of the link bandwidth. You might want to change that value if a different level of link utilization is required, or if the configured bandwidth does not match the actual link bandwidth and you want to adjust actual bandwidth of BEIGRP by command. To configure the percentage of bandwidth, use the following command in interface command of global configure directory:

Command	Purpose
<b>ip bepbandwidth-percent</b> <i>percent</i>	Configures the maximun percentage of bandwidth that may be used by BEIGRP on an interface.

[DEFAULT@Router /config/]#interface

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

08)Multilink Multilink-group interface

(09)Virtual-template Virtual template interface

(10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): 0

Note:here input interface type , FastEthernet is only an example..

Please input a interface name:f0/0

Note:here input interface name , f0/0 is only an example..

Will you excute it? (Y/N):y

Key Word:

Q(quit)

.....

(18)history look up history

(19)interface interface configuration

(20)ip IP configuration commands

(21)keepalive Enable keepalive

.....

Please Input the code of command to be excute(0-35):20 (Select IPCommand)

Key Word:

U(undo) D(default) Q(quit)

(00)access-group Specify access control for packets

(01)address IP address

(02)beigrp Enhanced Interior Gateway Routing Protocol

(03)directed-broadcast Enable forwarding of directed broadcasts

(04)fast-switch Fast-Switch interface commands

.....

(18)unnumbered Enable IP processing without an explicit address

(19)unreachables Enable sending ICMP Unreachable messages

Please Input the code of command to be excute(0-19): 2

input 2 , Select beigrp option :

Key Word:

Q(quit)

(00)bandwidth-percent Set BEIGRP bandwidth limit

(01)hello-interval Configures BEIGRP hello interval

(02)hold-time Configures BEIGRP hold time

(03)passive Suppress routing updates on an interface

(04)split-horizon Perform split horizon

(05)summary-address Perform address summarization

Please Input the code of command to be excute(0-5): 0

input 0 , Select bandwidth-percent option :

Key Word:

Q(quit)

(00)<1-999999> Maximum bandwidth percentage that BEIGRP may use

Please Input the code of command to be excute(0-0): 0

input 0 , Select <1-999999> option

Please input a digital number:Please input a string:23

Note:here input the maximum bandwidth percents , 23 is only an example..

Will you excute it? (Y/N):y

### 5.8.5 Adjusting the BEIGRP Calculating Coefficient of Metrics

Sometimes you need to adjust the BEIGRP calculating coefficient of `metrics` to finally effect the route selecting policy. Although BEIGRP default calculating coefficient have been carefully selected to provide excellent operation in most networks, you need to adjust the BEIGRP calculating coefficient. Adjusting BEIGRP calculating coefficient of metric can dramatically affect network performance, so the operation should be handled by the experienced engineer.

Command	Purpose
<code>metric weights k1 k2 k3 k4 k5</code>	Adjusts the BEIGRP calculating coefficient of <code>metrics</code>

Select metric

Key Word:

U(undo) D(default) Q(quit)

(00)weight Modify BEIGRP metric coefficients

Please Input the code of command to be excute(0-0): 0

input 0 , Select weight option

Key Word:

Q(quit)

(00)<0-4294967295> K1

Please Input the code of command to be excute(0-0): 0

input 0 , Select <0-4294967295> option

Please input a digital number:Please input a string:20

Note:here input coefficient K1 , 20 is only an example..

Key Word:

Q(quit)

(00)<0-4294967295> K2

Please Input the code of command to be excute(0-0): 0

input 0 , Select <0-4294967295> option

Please input a digital number:Please input a string:30

Note:here input coefficient K2 , 30 is only an example..

Key Word:

Q(quit)

(00)<0-4294967295> K3

Please Input the code of command to be excute(0-0): 0

input 0 , Select <0-4294967295> option

Please input a digital number:Please input a string:40

Note:here input coefficient K3 , 40 is only an example..

Key Word:

Q(quit)

(00)<0-4294967295> K4

Please Input the code of command to be excute(0-0): 0

input 0 , Select <0-4294967295> option

Please input a digital number:Please input a string:50

Note:here input coefficient K4 , 50 is only an example..

Key Word:

Q(quit)

(00)<0-4294967295> K5

Please Input the code of command to be excute(0-0): 0

input 0 , Select <0-4294967295> option

Please input a digital number:Please input a string:60

Note:here input coefficient K5 , 60 is only an example..

Will you excute it? (Y/N):y

### 5.8.6 Apply offset to Adjust Routing Metrics

With offset-list we can add all ingress and egress routes or the compound metric of some routes thereinto meeting the demand. The purpose we do that for is to finally affect the routing result and make it meet our expectations. In course of configuration you can specify access-list or application interface in offset-list as your demand in command to confirm the routes which need operation of adding offsets. Please look at commands below:

Command	Purpose
<code>offset-list {type number   *} {in   out} access-list-name offset</code>	Apply an offset-list

In the directory of configuring beigrp routing select `offset`

Key Word:

U(undo) D(default) Q(quit)

(00)interface-name

(01)\* All interface

Please Input the code of command to be excute(0-1): 0Please input a interface name:f0/0

Note:here input interface name , f0/0 is only an example..

Key Word:

Q(quit)

(00)in Filter incoming routing updates

(01)out Filter outgoing routing updates

Please Input the code of command to be excute(0-1): 0

**Note:**here you can Select according to you demands , in indicats applying access list to inbound routes, out indicats applying access list to outbound routs. Here select in is only an example..

Key Word:

Q(quit)

(00)WORD Name of access-list

Please Input the code of command to be excute(0-0): 0

input 0 , Select WORD option .

Please input a string:name

Note:here input the access list name , name is only an example..

Key Word:

Q(quit)

(00)<0-2147483647>-- offset

Please Input the code of command to be excute(0-0): 0

Please input a string:23

input an offset , 23 is only an example.

Will you excute it? (Y/N):y

### 5.8.7 Disabling Route Automatic Summarization

BEIGRP Route Auto-summary differs from other dynamic routing protocols and it obeys rules below:

- When a BEIGRP process defines multiple networks, summary route of a network will be created as long as the network has a subnet in BEIGRP topology-list.
- The created summary route will point to interface Null0 and have the minimal metric in all subnets of the network having summary route. Summary route will also be inserted into main IP routing table and its management metric is 5 (non-configured).
- When the router transmitting update to a neighbor of different IP network, subnets in rule 1 and rule 2 will be canceled and only summary route will be transmited.
- Subnet in any network not listed in definition of BEIGRP process won't be summed up.

In some cases you may want to inform every particular route to neighbors, here you can use command below:

Command	Purpose
<b>(undo) auto-summary</b>	Disables route automatic summarization.

In the directory of configuring beigrp route Select U(undo),

Key Word:

Q(quit)

(00)auto-summary Config automatic network number summarization

(01)beigrp config beigrp

...

Please Input the code of command to be excute(0-21): 0

Will you excute it? (Y/N):y

### 5.8.8 Customize Route Summary

When route auto-summary can't meet the requirement, you can configure route summary on every interface of processing

BEIGRP and appoint the objective network of processing summary. Interface configured with summary won't send any particular updating information belonging to subnets in this summary network segment, and other interfaces won't be affected.

Here the summary operation will obey rules below:

- After an interface is configured with summary, summary route of a network will be created as soon as this network has at least one subnet in BEIGRP topology list.
- The created summary route will point to interface Null0 and have the minimal metric in all particular routes contained in summary route. Summary route will also be inserted in main IP routing table and its administrative distance is 5 (non-configured).
- When the router transmitting update on interface configured with summary, particular routes belonging to summary segment will be canceled and the update sent to other interfaces won't be affected.

Command	Purpose
<b>ip beigrp</b> <i>process_id</i> <b>summary-address</b> <i>address mask</i>	Configure routing summary on interface.

[DEFAULT@Router /config/]#interface

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

(08)Multilink Multilink-group interface

(09)Virtual-template Virtual template interface

(10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): 0

input 0 , Select FastEthernet option :

Please input a interface name:f0/0

Note:here input interface name ,f0/0 is only an example..

Will you excute it? (Y/N):y

Key Word:

Q(quit)

.....

(17)help Description of the interactive help system

(18)history look up history

(19)interface interface configuration

(20)ip IP configuration commands

(21)keepalive Enable keepalive

.....

Please Input the code of command to be excute(0-35):20(Select IPCommand)

Key Word:

U(undo) D(default) Q(quit)

(00)access-group Specify access control for packets

(01)address IP address

```

(02)beigrp      Enhanced Interior Gateway Routing Protocol
(03)directed-broadcast Enable forwarding of directed broadcasts
(04)fast-switch Fast-Switch interface commands
.....
(18)unnumbered Enable IP processing without an explicit address
(19)unreachables Enable sending ICMP Unreachable messages
Please Input the code of command to be excute(0-19):2
input 2 , Select beigrp option
Key Word:
Q(quit)
(00)bandwidth-percent Set BEIGRP bandwidth limit
(01)hello-interval    Configures BEIGRP hello interval
(02)hold-time         Configures BEIGRP hold time
(03)passive           Suppress routing updates on an interface
(04)split-horizon     Perform split horizon
(05)summary-address   Perform address summarization
Please Input the code of command to be excute(0-5): 5
input 5 , Select summary-address option
Key Word:
Q(quit)
(00)A.B.C.D   IP Address
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option
Please input a IP Address:192.168.18.90
Note: here input summary route 的 Purpose 网段 , 192.168.18.90 is only an example..
Key Word:
Q(quit)
(00)A.B.C.D   Network mask
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option
Please input a IP Address:255.255.0.0
Note: here input network mask of the summary route , 255.255.0.0 is only an example..
Will you excute it? (Y/N):y

```

### 5.8.9 Configure Other BEIGRP Parameters

To adapt different network terms, to make BEIGRP more valid and function more efficiently, we may also be required to adjust some parameters below:

- Adjust BEIGRP with the interval of sending hello message and the overtime of neighbor life.
- Inactivate level division

### 5.8.10 Adjusting the BEIGRP Send Hello Packets Interval and Neighbor Out-time

Three objects required for BEIGRP hello protocol to achieve correct BEIGRP operation:

- It can find out new neighbors. Neighbor finding is automatic and without other manual configuration.
- It will validate the configurations of neighbors and allow communicating with only the neighbors configured with compatible mode.
- It will continuously monitor the availability of neighbors and detect the disappearance of neighbors.

Router will transmit hello multicast messages on all interfaces processing BEIGRP. Every router supporting BEIGRP will accept these multicast messages and then find out its neighbors.

Hello protocol detects disappearance of neighbors through two timers: Hello interval specifies the frequency of sending BEIGRP hello message on interface in router. And hold timer specifies the time the router will wait for communicating datas from a special neighbor and after the time the neighbor will be annouced dead. We provide that hold timer should be reset at every time when the router receives any kind of BEIGRP message from neighbor router.

Different default values of hello timer are used in networks of different types or different bandwidths:

Interface Type Packing		Hello Timer (second)	Hold Timer (second)
LAN Interface	Random	5	15
WAN Interface	HDLC or PPP	5	15
	NBMA interface, bandwidth<= T1	60	180
	NBMA interface, bandwidth > T1	5	15
	Point-to-point subinterface on NBMA interface	5	15

In Hello protocol the different default values of timers will cause the result that the BEIGRP neighbors connecting same IP subnet use different hello and hold timers. To resolve this problem, in hello messages of every router hold timer should be specified. Here every BEIGRP router uses hold timer specified in hello messages of its neighbor to judge the timeout of this neighbor. Thus we make the error detect timers of different neighbors present in different stations of the same WAN nephogram. But in some special cases the default values of timers can't meet our demands. So you can use command below if you want to adjust the interval of sending hello message:

Command	Purpose
<b>ip bephello-interval</b> <i>seconds</i>	Adjust the interval of sending hello message on the interface.

In the directory of configuring interface Command Select ip Command

Key Word:

U(undo) D(default) Q(quit)

(00)access-group Specify access control for packets

(01)address IP address

(02)beigrp Enhanced Interior Gateway Routing Protocol

(03)directed-broadcast Enable forwarding of directed broadcasts

(04)fast-switch Fast-Switch interface commands

.....

(18)unnumbered Enable IP processing without an explicit address

(19)unreachables Enable sending ICMP Unreachable messages

Please Input the code of command to be excute(0-19):2

input 2 , Select beigrp option

Key Word:

Q(quit)

(00)bandwidth-percent Set BEIGRP bandwidth limit

(01)hello-interval Configures BEIGRP hello interval

(02)hold-time Configures BEIGRP hold time

(03)passive Suppress routing updates on an interface

(04)split-horizon Perform split horizon

(05)summary-address Perform address summarization  
Please Input the code of command to be excute(0-5): 1  
input 1 , Select hello-interval option  
Key Word:  
Q(quit)  
(00)<1-65535> Seconds between hello transmissions  
Please Input the code of command to be excute(0-0): 0  
input 0 , Select <1-65535> option  
Please input a digital number:Please input a string:20  
Note:here input , 20 is only an example.  
Will you excute it? (Y/N):y

Use command below to adjust the overtime timer of neighbors:

Command	Purpose
<b>ip bephold-time</b> <i>seconds</i>	Adjust dead interval of neighbors.

In the directory of configuring interface Command Select ipCommand  
Key Word:  
U(undo) D(default) Q(quit)  
(00)access-group Specify access control for packets  
(01)address IP address  
(02)beigrp Enhanced Interior Gateway Routing Protocol  
(03)directed-broadcast Enable forwarding of directed broadcasts  
(04)fast-switch Fast-Switch interface commands  
.....  
(18)unnumbered Enable IP processing without an explicit address  
(19)unreachables Enable sending ICMP Unreachable messages  
Please Input the code of command to be excute(0-19):2  
input 2 , Select beigrp option  
Key Word:  
Q(quit)  
(00)bandwidth-percent Set BEIGRP bandwidth limit  
(01)hello-interval Configures BEIGRP hello interval  
(02)hold-time Configures BEIGRP hold time  
(03)passive Suppress routing updates on an interface  
(04)split-horizon Perform split horizon  
(05)summary-address Perform address summarization  
Please Input the code of command to be excute(0-5): 2  
input 2 , Select hold-time option  
Key Word:  
Q(quit)  
(00)<1-65535> Seconds before neighbor is considered down  
Please Input the code of command to be excute(0-0): 0  
input 0 , Select <1-65535> option  
Please input a digital number:Please input a string:30  
Note:here input the timeout , 30 is only an example.  
Will you excute it? (Y/N):y

### 5.8.11 Disabling Horizontal Split

In normal case we want to use horizontal split which will forbid the routing information got from an interface to be broadcasted from the same interface. Thus we can avoid routing loop. But in some cases this action is not optimal and we can use command below to inactivate horizontal split:

Command	Purpose
<b>Ip (undo) beigrp split-horizon</b>	Disable horizontal split

In the directory of configuring interface Select ipCommand

Key Word:

```
U(undo) D(default) Q(quit)
(00)access-group Specify access control for packets
(01)address IP address
(02)beigrp Enhanced Interior Gateway Routing Protocol
(03)directed-broadcast Enable forwarding of directed broadcasts
.....
Please Input the code of command to be excute(0-19): u
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)access-group Specify access control for packets
(01)address IP address
(02)beigrp Enhanced Interior Gateway Routing Protocol
(03)directed-broadcast Enable forwarding of directed broadcasts
.....
Please Input the code of command to be excute(0-19): 2
```

Key Word:

```
Q(quit)
(00)bandwidth-percent Set BEIGRP bandwidth limit
(01)hello-interval Configures BEIGRP hello interval
(02)hold-time Configures BEIGRP hold time
(03)passive Suppress routing updates on an interface
(04)split-horizon Perform split horizon
(05)summary-address Perform address summarization
Please Input the code of command to be excute(0-5): 4
Will you excute it? (Y/N):y
```

### 5.8.12 Monitor and Maintain BEIGRP

Use command below to clear neighborliness of neighbors:

Command	Purpose
<b>clear ip beigrp neighbors</b> [ <i>as-number</i>   <i>interface</i> ]	Clear neighborliness of neighbors.

```
[DEFAULT@Router /enable/]#clear
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)arp-cache Clear the entire ARP cache
```

```
(01)dialer Clear dialer statistics
(02)frame-relay-inarp Clear inverse ARP entries from the map table
(03)ip IP
(04)l2tp L2TP tunnel or session
.....
(10)telnet Clear incoming telnet connection
(11)x25 Clear X.25 circuits
Please Input the code of command to be excute(0-11): 3
```

input 3 , Select ip option :

Key Word:

```
Q(quit)
(00)beigrp Clear BEIGRP
(01)bgp BGP information
(02)dhcpd DHCP Server information
(03)fast-switch Clear FSC
(04)nat Clear NAT
(05)prefix-list Prefix list information
Please Input the code of command to be excute(0-5): 0
```

input 0 , Select beigrp option

Key Word:

```
Q(quit)
(00)<1-65535> AS Number
(01)neighbors Clear BEIGRP neighbors
Please Input the code of command to be excute(0-1): 1
```

input 1 , Select neighbors option

Key Word:

```
Q(quit)
(00)A.B.C.D clear BEIGRP neighbors
(01)interface-name
(02)<cr>
Please Input the code of command to be excute(0-2): 0
```

Note:here you can Select according to your demands , A.B.C.D indicates clearing all EIGRP neighbor addresses ; interface-name indicates interface 的名称 ,input this parameter ,all neighbors on the interface will process neighbor reset ;here Select A.B.C.D is only an example.

Please input a IP Address:192.168.19.80

Note: As to different options ,there are different input prompts.here input 192.168.19.80 is only an example. .  
Will you excute it? (Y/N):y

Use commands below to display various BEIGRP statistic information:

Command	Purpose
---------	---------

<b>show ip beigrp interfaces</b> [ <i>interface</i> ] [ <i>as-number</i> ]	Display information of BEIGRP interfaces.
<b>show ip beigrp neighbors</b> [ <i>as-number</i>   <i>interface</i> ]	Display information of BEIGRP neighbors.
<b>show ip beigrp topology</b> [ <i>as-number</i>   <b>all-link</b>   <b>summary</b>   <b>active</b> ]	Display information of BEIGRP topology list.

Command	Purpose
<b>show ip beigrp interfaces</b> [ <i>interface</i> ] [ <i>as-number</i> ]	display BEIGRP interface information

[DEFAULT@Router /enable/]#show

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command

(01)arp ARP table

.....

(17)interface interface status and configuration

(18)ip IP information

(19)job Job parameters and statistics

(20)l2tp L2TP information

--More--

**18**

input 18 , Select ip option

Key Word:

Q(quit)

(00)access-lists List IP access lists

(01)as-path-list Information of AS-Path list

(02)beigrp Show BEIGRP information

(03)bgp BGP information

(04)cache IP route cache

(05)community-list Information of community-list

(06)dhcpd DHCP Server information

(07)fast-switch Fast-switch information

(08)interface IP interface status and configuration

.....

--More--

**2**

input 2 , Select beigrp option

Key Word:

Q(quit)

(00)interface Show BEIGRP interface

(01)neighbors Show BEIGRP neighbor

(02)topology Show BEIGRP Topology Table

(03)traffic BEIGRP Traffic Statistics

(04)protocols IP routing protocol process parameters and statistics

Please Input the code of command to be excute(0-4): 0

input 0 , Select interface option

Key Word:

Q(quit)

(00)<1-65535> AS Number

(01)interface-name

(02)<cr>

Please Input the code of command to be excute(0-2): 0

Note:as-number indicates the autonomous system number , If you have specified this parameter , it will only display neighbors of this EIGRP course ; interface indicates interface name , If you have specified this parameter , it will only display EIGRP neighbors on this interface.here Select as-number is only an example..

Please input a digital number:Please input a string:23

Note:here please input according to the prompt , 23 is only an example..

Will you excute it? (Y/N):y

It will display information as below :

BEIGRP interfaces for process 23

Interface Peers Flags Xmit Queue Mean SRTT Pacing Time

(Un/Reliable) (10ms) (10ms)

Command	Purpose
<b>show ip beigrp neighbors</b> [ <i>as-number</i>   <i>interface</i> ]	display BEIGRP neighbor information

[DEFAULT@Router /enable/]#show

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command

(01)arp ARP table

.....

(17)interface interface status and configuration

(18)ip IP information

(19)job Job parameters and statistics

(20)l2tp L2TP information

--More--

**18**

input 18 , Select ip option

Key Word:

Q(quit)

(00)access-lists List IP access lists

(01)as-path-list Information of AS-Path list

(02)beigrp Show BEIGRP information

(03)bgp BGP information

(04)cache IP route cache

(05)community-list Information of community-list

(06)dhcpd DHCP Server information

(07)fast-switch Fast-switch information

(08)interface IP interface status and configuration

.....

--More--

**2**

input 2 , Select beigrp option

Key Word:

Q(quit)

(00)interface Show BEIGRP interface

(01)neighbors Show BEIGRP neighbor

- (02)topology Show BEIGRP Topology Table
- (03)traffic BEIGRP Traffic Statistics
- (04)protocols IP routing protocol process parameters and statistics

Please Input the code of command to be excute(0-4): 1

input 1 ,Select neighbors option

Key Word:

Q(quit)

(00)<1-65535> AS Number

(01)interface-name

(02)detail Show detail peer information

(03)<cr>

Please Input the code of command to be excute(0-3): 0

Note:as-number indicates autonomous system number ,If you specify this parameter ,it will only display neighbors of thisEIGRP course ; interface indicates interface name , If you specify this parameter , it will only display EIGRP neighbor on this interface ; detail indicates display detailed neighbor information .here Select as-number is only an example..

Please input a digital number:Please input a string:23

Note: please input according to prompt ,here input 23 is only an example.

Key Word:

Q(quit)

(00)detail Show detail peer information

(01)<cr>

Please Input the code of command to be excute(0-1): 0

Note: please input according to prompt ,here input detail is only an example.

Will you excute it? (Y/N):y

It will display information as below :

IP-BEIGRP neighbors for process 23

Address interface hold uptime srtt rto Q\_cnt Seq

(sec) (10ms)(10ms)

Command	Purpose
<b>show ip beigrp topology</b> [ <i>as-number</i>   <b>all-link</b>   <b>summary</b>   <b>active</b> ]	display BEIGRP topology information

[DEFAULT@Router /enable/]#show

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command

(01)arp ARP table

.....

(17)interface interface status and configuration

(18)ip IP information

(19)job Job parameters and statistics

(20)l2tp L2TP information

--More--

**18**

input 18 , Select ip option

Key Word:

Q(quit)

(00)access-lists List IP access lists

```
(01)as-path-list Information of AS-Path list
(02)beigrp Show BEIGRP information
(03)bgp BGP information
(04)cache IP route cache
(05)community-list Information of community-list
(06)dhcpd DHCP Server information
(07)fast-switch Fast-switch information
(08)interface IP interface status and configuration
.....
--More--
```

2

input 2 , Select beigrp option

Key Word:

Q(quit)

```
(00)interface Show BEIGRP interface
(01)neighbors Show BEIGRP neighbor
(02)topology Show BEIGRP Topology Table
(03)traffic BEIGRP Traffic Statistics
(04)protocols IP routing protocol process parameters and statistics
```

Please Input the code of command to be excute(0-4): 2

input 2 , Select topology option

Key Word:

Q(quit)

```
(00)<1-65535> AS Number
(01)A.B.C.D Network for display information about
(02)active Show only active entries
(03)all-links Show all links in topology table
(04)pending Show only entries pending transmission
(05)summary Show all summary route in the topology table
(06)zero-successors Show only zero successor entries
(07)<cr>
```

Please Input the code of command to be excute(0-7): 0

Note : Select as your demands , as number is only an example.

Please input a digital number:Please input a string:23

Note : input according different prompt , 23 is only an example.

Key Word:

Q(quit)

```
(00)active Show only active entries
(01)all-links Show all links in topology table
(02)pending Show only entries pending transmission
(03)summary Show all summary route in the topology table
(04)zero-successors Show only zero successor entries
(05)<cr>
```

Please Input the code of command to be excute(0-5): 0

Note : input according different prompt , active is only an example.

Will you excute it? (Y/N):y

It will display information as below:

IP BEIGRP Topology Table for AS(23)/ID(0.0.0.0)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  
r - reply Status, s - sia Status

### 5.8.13 BEIGRP Configuration Example

#### Examples of Routing Summarization

The example below will configure the summary route of sending 10.0.0.0/8 on ethernet1/1, and all subnet routes belonging to the segment won't be informed to neighbors. Here we inactivate auto-summarization of BEIGRP process.

```
interface Ethernet 1/1
ip beigrp summary-address 1 10.0.0.0 255.0.0.0
!
router beigrp 1
network 172.16.0.0 255.255.0.0
(undo)auto-summary
```

### 5.9 Configuring OSPF Task List

#### 5.9.1 Configuring OSPF

This chapter describes how to configure Open Shortest Path First (OSPF). For a complete description of the OSPF commands in this chapter, refer to the "OSPF Commands" chapter.

OSPF is an Interior Gateway Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). Designed expressly for IP networks, OSPF supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

#### 5.9.2 The D-Link Router OSPF Implementation

The D-Link implementation conforms to the OSPF Version 2 specifications detailed in the Internet RFC 2328. The list that follows outlines key features supported in the D-Link OSPF implementation:

1. Stub areas—Definition of stub areas is supported.
2. Route redistribution—Routes learned via any IP routing protocol can be redistributed into any other IP routing protocol. At the intradomain level, OSPF can import routes learned via Interior Gateway Routing Protocol (IGRP), Routing Information Protocol (RIP), and Intermediate System-to-Intermediate System (IS-IS). OSPF routes can also be exported into IGRP, RIP, and IS-IS. At the interdomain level, OSPF can import routes learned via Exterior Gateway Protocol (EGP) and Border Gateway Protocol (BGP). OSPF routes can be exported into BGP and EGP.
3. Authentication—Plain text and Message Digest 5 (MD5) authentication among neighboring routers within an area is supported.
4. Routing interface parameters—Configurable parameters supported include interface output cost, retransmission interval, interface transmit delay, router priority, router "dead" and hello intervals, and authentication key.
5. Virtual links—Virtual links are supported.
6. Not so stubby area (NSSA)—RFC 1587.
7. OSPF over demand circuit—RFC 1793.

#### 5.9.3 OSPF Configuration Task List

OSPF typically requires coordination among many internal routers: Area Border Routers (ABRs), which are routers connected to multiple areas, and Autonomous System Boundary Routers (ASBRs). At a minimum, OSPF-based routers or

access servers can be configured with all default parameter values, no authentication, and interfaces assigned to areas. If you intend to customize your environment, you must ensure coordinated configurations of all routers.

To configure OSPF, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional, but might be required for your application.

1. Enabling OSPF
2. Configuring OSPF Interface Parameters
3. Configuring OSPF over Different Physical Networks
4. Configuring OSPF Area Parameters
5. Configuring OSPF NSSA Area
6. Configuring Route Summarization Between OSPF Areas
7. Configuring Route Summarization When Redistributing Routes into OSPF
8. Creating Virtual Links
9. Generating a Default Route
10. Configuring Route for Lookup of DNS Names
11. Forcing the Router ID Choice with a Loopback Interface
12. Configuring the OSPF Administrative Distances
13. Configuring Route Calculation Timers
14. Start the Configuring of On-Demand Link
15. Monitoring and Maintaining OSPF

In addition, you can specify route redistribution; see the task "Redistribute Routing Information" in the chapter "Configuring IP Routing Protocol-Independent Features" for information on how to configure route redistribution.

### 5.9.4 Enabling OSPF

As with other routing protocols, enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses. To do so, use the following commands beginning in global configuration directory:

Step	Command	Purpose
1	<b>router ospf</b> <i>process-id</i>	Enables OSPF routing, which places you in router configuration mode.
2	<b>network</b> <i>address mask area area-id</i>	Defines an interface on which OSPF runs and define the area ID for that interface.

Step1 :

input routerCommand , prompt:

```
(00)beigrp      Enable BEIGRP (compatible with eigrp)
(01)bgp         Enable Border Gateway Protocol (BGP)
(02)ospf        Enable Open Shortest Path First (OSPF)
(03)rip         Enable Routing Information Protocol(RIP)
```

Please Input the code of command to be excute(0-3): 2

input 2 , Select ospf option , prompt is as below:

```
(00)<1-65535>   Process ID
```

Please Input the code of command to be excute(0-0): 0

input 0 , prompt is as below:

Please input a digital number:Please input a string:

input process-id.

Step2 :

In the prompt Select 14 option , prompt is as below:

(00)A.B.C.D            Network number

Please Input the code of command to be excute(0-0): 0

input 0 , Select A.B.C.D option , prompt is as below:

Please input a IP Address:

input IP , then prompt is as below:

(00)A.B.C.D            OSPF network mask

Please Input the code of command to be excute(0-0): 0

input 0 , Select A.B.C.D option , prompt is as below:

Please input a IP Address:

input mask , then prompt is as below:

(00)area            Set the OSPF area ID

Please Input the code of command to be excute(0-0): 0

input 0 , Select area option , then input area-id.

## 5.9.5 Configuring OSPF Interface Parameters

D-Link OSPF implementation allows you to alter certain interface-specific OSPF parameters, as needed. You are not required to alter any of these parameters, but some interface parameters must be consistent across all routers in an attached network.

To specify interface parameters for your network, use the following commands in interface configuration mode:

Command	Purpose
<b>ip ospf cost</b> <i>cost</i>	Explicitly specifies the cost of sending a packet on an OSPF interface.
<b>ip ospf retransmit-interval</b> <i>seconds</i>	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.
<b>ip ospf transmit-delay</b> <i>seconds</i>	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.
<b>ip ospf priority</b> <i>number</i>	Sets priority to help determine the OSPF designated router for a network.
<b>ip ospf hello-interval</b> <i>seconds</i>	Specifies the length of time between the hello packets that sends on an OSPF interface.
<b>ip ospf dead-interval</b> <i>seconds</i>	Sets the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet.
<b>ip ospf authentication-key</b> <i>key</i>	Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication.
<b>ip ospf message-digest-key</b> <i>keyid md5 key</i>	Enables OSPF MD5 authentication.
<b>ip ospf passive</b>	Do not send a hello packet in the port.

Take the first command for an example. :

In the prompt Select 18 option , prompt is as below:

```
(00)access-group          Specify access control for packets
    .....
(10)ospf                  set OSPF parameter for this port
    .....
```

Please Input the code of command to be excute(0-18): 10

input 10 , Select ospf option , prompt is as below:

```
(00)cost                  Interface cost
(01)dead-interval        Interval after which a neighbor is declared dead
(02)demand-circuit       OSPF Demand Circiut
    .....
```

Please Input the code of command to be excute(0-10): 0

input 0 , Select cost option , prompt:

```
(00)<1-65535>            Interface cost value
```

Please Input the code of command to be excute(0-0): 0

input 0 , then prompt is as below:

Please input a digital number:Please input a string:

```
input  cost value
```

### 5.9.6 Configuring OSPF over Different Physical Networks

OSPF classifies different media into the following three types of networks by default:

1. Broadcast networks (Ethernet, Token Ring, and FDDI)
2. Nonbroadcast multiaccess (NBMA) networks (Switched Multimegabit Data Service (SMDS), Frame Relay, and X.25)
3. Point-to-point networks (High-Level Data Link Control [HDLC], PPP)

You can configure your network as either a broadcast or an NBMA network.

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. Refer to the x25 map and frame-relay map command descriptions in the Wide-Area Networking Command Reference publication for more detail.

### 5.9.7 Configuring Your OSPF Network Type

You have the choice of configuring your OSPF network type as either broadcast or NBMA, regardless of the default media type. Using this feature, you can configure broadcast networks as NBMA networks when, for example, you have routers in your network that do not support multicast addressing. You also can configure NBMA networks (such as X.25, Frame Relay, and SMDS) as broadcast networks. This feature saves you from needing to configure neighbors, as described in the section "Configuring OSPF for Nonbroadcast Networks" later in this chapter.

Configuring NBMA, multiaccess networks as either broadcast or nonbroadcast assumes that there are virtual circuits (VCs) from every router to every router or fully meshed network. This is not true for some cases, for example, because of cost constraints, or when you have only a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers not directly connected will go through the router that has VCs to both routers.

An OSPF point-to-multipoint interface is defined as a numbered point-to-point interface having one or more neighbors. It creates multiple host routes. An OSPF point-to-multipoint network has the following benefits compared to NBMA and point-to-point networks:

- Point-to-multipoint is easier to configure because it requires no configuration of neighbor commands, it consumes only one IP subnet, and it requires no designated router election.
- It costs less because it does not require a fully meshed topology.
- It is more reliable because it maintains connectivity in the event of VC failure.

To configure your OSPF network type, use the following command in interface configuration mode:

Command	Purpose
<b>ip ospf network {broadcast   non-broadcast   point-to-multipoint [non-broadcast] }</b>	Configures the OSPF network type for a specified interface.

In the prompt Select 18 option , It will list all arguments :

```
(00)access-group          Specify access control for packets
```

```
.....
```

```
(10)ospf                  set OSPF parameter for this port
```

```
.....
```

Please Input the code of command to be excute(0-18): 10

input 10 ,Select ospf option ,prompt is as below:

```
(00)cost                  Interface cost
```

```
.....
```

```
(05)network              Network type
```

```
.....
```

Please Input the code of command to be excute(0-10): 5

input 5 ,Select network option ,prompt is as below:

```
(00)broadcast            Set to broadcast
```

```
(01)non-broadcast        Set to non-broadcast
```

```
(02)point-to-multipoint Set to point-to-multipoint
```

```
(03)point-to-point       Set to point-to-point
```

Please Input the code of command to be excute(0-3):

Select network type .

See the end of this chapter for an example of an OSPF point-to-multipoint network.

### 5.9.8 Configuring Point-to-Multipoint, Broadcast Networks

On point-to-multipoint, broadcast networks, there is no need to specify neighbors. However, you can specify neighbors with the neighbor router configuration command, in which case you should specify a cost to that neighbor.

Before the point-to-multipoint keyword was added to the ip ospf network interface configuration command, some OSPF point-to-multipoint protocol traffic was treated as multicast traffic. Therefore, the neighbor router configuration command was not needed for point-to-multipoint interfaces because multicast took care of the traffic. Hello, update, and acknowledgment messages were sent using multicast. In particular, multicast hello messages discovered all neighbors dynamically.

On any point-to-multipoint interface (broadcast or not), the router assumed that the cost to each neighbor was equal. The cost was configured with the ip ospf cost interface configuration command. In reality, the bandwidth to each neighbor is different, so the cost should differ. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

To treat an interface as point-to-multipoint broadcast and assign a cost to each neighbor, use the following commands beginning in interface configuration mode:

Step	Command	Purpose
1	<b>ip ospf network point-to-multipoint</b>	Configure an interface as point-to-multipoint for broadcast media.
2	<b>exit</b>	Enter global configuration mode.
3	<b>router ospf <i>process-id</i></b>	Configure an OSPF routing process and enter router configuration mode.
4	<b>neighbor <i>ip-address cost number</i></b>	Specify a neighbor and assign a cost to the neighbor.
5		Repeat Step 4 for each neighbor if you want to specify a cost. Otherwise, neighbors will assume the cost of the interface, based on the ip ospf cost command.

**Step1 :**

In the prompt Select 18 option , it will list all arguments :

```
(00)access-group          Specify access control for packets
```

```
.....
```

```
(10)ospf                  set OSPF parameter for this port
```

```
.....
```

Please Input the code of command to be excute(0-18): 10

input 10 ,Select ospf option , prompt is as below:

```
(00)cost                  Interface cost
```

```
.....
```

```
(05)network              Network type
```

```
.....
```

Please Input the code of command to be excute(0-10): 5

input 5 ,Select network option , prompt is as below:

```
(00)broadcast            Set to broadcast
```

```
(01)non-broadcast        Set to non-broadcast
```

```
(02)point-to-multipoint Set to point-to-multipoint
```

```
(03)point-to-point       Set to point-to-point
```

Please Input the code of command to be excute(0-3): 2

input 2 ,Select point-to-multipoint option , prompt is as below:

```
(00)broadcast            Point-to-multipoint with broadcast (default)
```

```
(01)non-broadcast        Point-to-multipoint with non-broadcast
```

```
(02)<cr>
```

Please Input the code of command to be excute(0-2): 0

input 0 ,Select broadcast option .

**Step2 :**

input exit Command ,enter into the global configure directory .

**Step3 :**

input router Command ,prompt is as below:

```
(00)beigrp               Enable BEIGRP (compatible with eigrp)
```

```
(01)bgp                  Enable Border Gateway Protocol (BGP)
```

```
(02)ospf                 Enable Open Shortest Path First (OSPF)
```

```
(03)rip                  Enable Routing Information Protocol(RIP)
```

Please Input the code of command to be excute(0-3): 2

input 2 , Select ospf option , prompt is as below:

```
(00)<1-65535>      Process ID
Please Input the code of command to be excute(0-0): 0
input 0 , prompt is as below:
Please input a digital number:Please input a string:
input process-id.
```

Step4 :

In the prompt Select 13 option , prompt is as below:

```
(00)A.B.C.D          Neighbor address
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option , prompt is as below:
Please input a IP Address:
input IP , then prompt is as below:
(00)cost             OSPF cost for point-to-multipoint neighbor
(01)poll-interval    OSPF dead-router polling interval
(02)priority         OSPF priority of non-broadcast neighbor
(03)<cr>
Please Input the code of command to be excute(0-3): 0
input 0 , Select cost option , prompt is as below:
(00)<0-65535> metrics
Please Input the code of command to be excute(0-0): 0
input 0 , then prompt is as below:
Please input a digital number:Please input a string:
input cost value , then prompt is as below:
(00)<cr>
Please Input the code of command to be excute(0-0): 0
input 0.
```

Step5 :

Repeat Step4 for every neighbor needing weight. Otherwisethe neighbor will use the weight specified by command ip ospf cost .

### 5.9.9 Configuring OSPF for Nonbroadcast Networks

Because there might be many routers attached to an OSPF network, a designated router is select ed for the network. It is necessary to use special configuration parameters in the designated router select ion if broadcast capability is not configured.

These parameters need only be configured in those devices that are themselves eligible to become the designated router or backup designated router (in other words, routers with a nonzero router priority value).

To configure routers that interconnect to nonbroadcast networks, use the following command in router configuration mode:

Command	Purpose
<b>neighbor</b> <i>ip-address</i> [ <b>priority</b> <i>number</i> ] [ <b>poll-interval</b> <i>seconds</i> ]	Configure a router interconnecting to nonbroadcast networks.

In the prompt Select 13 option , then prompt is as below:

```

(00)A.B.C.D           Neighbor address
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option , prompt is as below:
Please input a IP Address:
input IP , then prompt is as below:
(00)cost             OSPF cost for point-to-multipoint neighbor
(01)poll-interval   OSPF dead-router polling interval
(02)priority        OSPF priority of non-broadcast neighbor
(03)<cr>
Please Input the code of command to be excute(0-3): 2
input 2 , Select priority option , prompt is as below:
(00)<0-255>          Priority
Please Input the code of command to be excute(0-0): 0
input 0 , then prompt is as below:
Please input a digital number:Please input a string:
input number value , prompt is as below:
(00)poll-interval   OSPF dead-router polling interval
(01)<cr>
Please Input the code of command to be excute(0-1): 0
input 0 , Select poll-interval option , prompt is as below:
(00)<0-4294967295>  seconds
Please Input the code of command to be excute(0-0): 0
input 0 , prompt is as below:
Please input a digital number:Please input a string:
input sencods value , then prompt is as below:
(00)<cr>
Please Input the code of command to be excute(0-0): 0
Select 0 and confirm it.

```

You can specify the following neighbor parameters, as required:

1. Priority for a neighboring router
2. Nonbroadcast poll interval
3. Reachable neighbor interface

On point-to-multipoint, nonbroadcast networks, you now use the *config-neighbor* command to identify neighbors. Assigning a cost to a neighbor is optional.

In the previous versions, some customers were using point-to-multipoint on nonbroadcast media (such as classic IP over ATM), so their routers could not dynamically discover their neighbors. This feature allows the *config-neighbor* command to be used on point-to-multipoint interfaces.

On any point-to-multipoint interface (broadcast or not), the router assumed the cost to each neighbor was equal. The cost was configured with the *config-ip ospf cost* command. In reality, the bandwidth to each neighbor is different, so the cost should differ. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

To treat the interface as point-to-multipoint when the media does not support broadcast, use the following commands beginning in interface configuration mode:

Step	Command	Purpose
1	<b>ip ospf network point-to-multipoint non-broadcast</b>	Configure an interface as point-to-multipoint for nonbroadcast media.
2	<b>exit</b>	Enter global configuration mode.
3	<b>router ospf <i>process-id</i></b>	Configure an OSPF routing process and enter router configuration mode.
4	<b>neighbor <i>ip-address</i> [<i>cost number</i>]</b>	Specify an OSPF neighbor and optionally assign a cost to the neighbor.
5		Repeat Step 4 for each neighbor.

Step1 :

In the prompt Select 18 option , , it will list all arguments :

(00)access-group            Specify access control for packets

.....

(10)ospf                    set OSPF parameter for this port

.....

Please Input the code of command to be excute(0-18): 10

input 10 , Select ospf option , prompt is as below:

(00)cost                    Interface cost

.....

(05)network                Network type

.....

Please Input the code of command to be excute(0-10): 5

input 5 , Select network option , prompt is as below:

(00)broadcast              Set to broadcast

(01)non-broadcast         Set to non-broadcast

(02)point-to-multipoint    Set to point-to-multipoint

(03)point-to-point         Set to point-to-point

Please Input the code of command to be excute(0-3): 2

input 2 , Select point-to-multipoint option , prompt is as below:

(00)broadcast              Point-to-multipoint with broadcast (default)

(01)non-broadcast         Point-to-multipoint with non-broadcast

(02)<cr>

Please Input the code of command to be excute(0-2): 1

input 1 , Select non-broadcast option .

Step2 :

input exit Command , enter into the global configure directory .

Step3 :

input router Command , prompt is as below:

(00)beigrp                 Enable BEIGRP (compatible with eigrp)

(01)bgp                    Enable Border Gateway Protocol (BGP)

(02)ospf                  Enable Open Shortest Path First (OSPF)

(03)rip                    Enable Routing Information Protocol(RIP)

Please Input the code of command to be excute(0-3): 2

input 2 , Select ospf option , prompt is as below:

(00)<1-65535>            Process ID

Please Input the code of command to be excute(0-0): 0  
input 0 , prompt is as below:  
Please input a digital number:Please input a string:  
input process-id.

Step4 :

In the prompt Select 13 option , prompt is as below:

(00)A.B.C.D Neighbor address  
Please Input the code of command to be excute(0-0): 0  
input 0 , Select A.B.C.D option , prompt is as below:  
Please input a IP Address:  
input IP , then prompt is as below:  
(00)cost OSPF cost for point-to-multipoint neighbor  
(01)poll-interval OSPF dead-router polling interval  
(02)priority OSPF priority of non-broadcast neighbor  
(03)<cr>

Please Input the code of command to be excute(0-3): 0  
input 0 , Select cost option , prompt is as below:

(00)<0-65535> metrics

Please Input the code of command to be excute(0-0): 0  
input 0 , then prompt is as below:

Please input a digital number:Please input a string:  
input cost value , then prompt is as below:

(00)<cr>

Please Input the code of command to be excute(0-0): 0  
input 0 and confirm it.

Step5 :

Repeat Step4 for each neighbor.

### 5.9.10 Configuring OSPF Area Parameters

The router allows you to configure several area parameters. These area parameters, shown in the following table, include authentication, defining stub areas, and assigning specific costs to the default summary route. Authentication allows password-based protection against unauthorized access to an area.

Stub areas are areas into which information on external routes is not sent. Instead, there is a default external route generated by the area border router, into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, default routing must be used in the stub area. To further reduce the number of LSAs sent into a stub area, you can configure no-summary on the ABR to prevent it from sending summary link advertisement (LSAs Type 3) into the stub area.

To specify an area parameter as needed for your network, use the following commands in router configuration mode:

Command	Purpose
<b>area <i>area-id</i> authentication simple</b>	Enable authentication for an OSPF area.
<b>area <i>area-id</i> authentication message-digest</b>	Enable MD5 authentication for an OSPF area.
<b>area <i>area-id</i> stub [no-summary]</b>	Define an area to be a stub area.
<b>area <i>area-id</i> default-cost <i>cost</i></b>	Assign a specific cost to the default summary route used for the stub area.

Take the first command for an example. :

In the prompt Select 0 option , prompt is as below:

```
(00)<0-4294967295>      OSPF area ID as a decimal value
(01)A.B.C.D            OSPF area ID in IP address format
Please Input the code of command to be excute(0-1): 0
input 0 , prompt is as below:
Please input a digital number:Please input a string:
input area-id value , then prompt is as below:
(00)authentication      Enable authentication
(01)default-cost        Set the summary default-cost of a NSSA/Stub area
(02)nssa                Specify a NSSA area
.....
Please Input the code of command to be excute(0-4): 0
input 0 , Select authentication option , prompt is as below:
(00)message-digest      Use message-digest authentication
(01)simple               Use simple authentication
Please Input the code of command to be excute(0-1): 1
input 1 , Select simple option and confirm it.
```

### 5.9.11 Configuring Route Summarization In OSPF Area

This feature causes a single summary route to be advertised to other areas by an ABR. In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

To specify an address range, use the following command in router configuration mode:

Command	Purpose
<b>area</b> <i>area-id</i> <b>range</b> <i>address mask</i>	Specify an address range for route of summarization.

In the prompt Select 0 option , prompt is as below:

```
(00)<0-4294967295>      OSPF area ID as a decimal value
(01)A.B.C.D            OSPF area ID in IP address format
Please Input the code of command to be excute(0-1): 0
input 0 , prompt is as below:
Please input a digital number:Please input a string:
input area-id value , then prompt is as below:
(00)authentication      Enable authentication
(01)default-cost        Set the summary default-cost of a NSSA/Stub area
(02)nssa                Specify a NSSA area
(03)range              Summarize LS_SUM_NET (border routers only)
.....
Please Input the code of command to be excute(0-4): 3
input 3 , Select range option , prompt is as below:
(00)A.B.C.D            IP address for match network
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option , prompt is as below:
```

Please input a IP Address:  
input IP ,  
(00)A.B.C.D IP address mask for match network  
Please Input the code of command to be excute(0-0): 0  
input 0 , Select A.B.C.D option , prompt is as below:  
Please input a IP Address:  
input mask , then prompt is as below:  
(00)advertise Advertise this range ( default )  
(01)not-advertise DoNotAdvertise this range  
(02)<cr>  
Please Input the code of command to be excute(0-2): 2  
input 2 and cofirm it.

### 5.9.12 Configuring Route Summarization When Redistributing Routes into OSPF

When routes from other protocols are redistributed into OSPF, each route is advertised individually in an external LSA. However, you can configure the D-Link router to advertise a single route for all the redistributed routes that are covered by a specified network address and mask. Doing so helps decrease the size of the OSPF link-state database.

To configure route summarization, use the following command in router configuration mode:

Command	Purpose
<b>summary-address</b> <i>prefix mask</i> <b>[not advertise]</b>	Specify an address and mask that covers redistributed routes, so only one summary route is advertised.

In the prompt Select 20 option , then prompt is as below:

(00)A.B.C.D IP summary address  
Please Input the code of command to be excute(0-0): 0  
input 0 , Select A.B.C.D option , prompt is as below:  
Please input a IP Address:  
input address , prompt is as below:  
(00)A.B.C.D Summary mask  
Please Input the code of command to be excute(0-0): 0  
input 0 , Select A.B.C.D option , prompt is as below:  
Please input a IP Address:  
input mask , prompt is as below:  
(00)not-advertise Do not advertise when translating OSPF type-7 LSA  
(01)<cr>  
Please Input the code of command to be excute(0-1):  
Select parameter and confirm it.

### 5.9.13 Generate a Default Route

You can force an autonomous system boundary router to generate a default route into an OSPF routing domain. Whenever you specifically configure redistribution of routes into an OSPF routing domain, the router automatically becomes an autonomous system boundary router. However, an autonomous system boundary router does not, by default, generate a default route into the OSPF routing domain.

To force the autonomous system boundary router to generate a default route, use the following command in router configuration mode:

Command	Purpose
<b>default-information originate</b> [always] [route-map <i>map-name</i> ]	Force the autonomous system boundary router to generate a default route into the OSPF routing domain.

In the prompt Select 4 option , prompt is as below:  
 (00)originate           Distribute a default route  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select originate option , prompt is as below:  
 (00)always            Always advertise default route  
 (01)route-map        Route-map reference  
 (02)<cr>  
 Please Input the code of command to be excute(0-2):  
 Select parameter and confirm it.

### 5.9.14 Force the Router ID Choice with a Loopback Interface

OSPF uses the largest IP address configured on the interfaces as its router ID. If the interface associated with this IP address is ever brought down, or if the address is removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces.

If a loopback interface is configured with an IP address, the router will use this IP address as its router ID, even if other interfaces have larger IP addresses. Since loopback interfaces never go down, greater stability in the routing table is achieved.

OSPF automatically prefers a loopback interface over any other kind, and it chooses the highest IP address among all loopback interfaces. If no loopback interfaces are present, the highest IP address in the router is chosen. You cannot tell OSPF to use any particular interface.

To configure an IP address on a loopback interface, use the following commands, starting in global configuration directory:

Step	Command	Purpose
1	<b>interface loopback 0</b>	Create a loopback interface, which places you in interface configuration mode.
2	<b>ip addr</b> <i>ip-address mask</i>	Assign an IP address to this interface.

Step1 :  
 input interface Command , prompt is as below:  
 (00)FastEthernet      FastEthernet interface  
 .....  
 (05)Loopback         Loopback interface  
 .....  
 Please Input the code of command to be excute(0-10): 5  
 input 5 , Select Loopback option , then prompt is as below:  
 Please input a interface name:loopback 0  
 input loopback 0.

Step2 :

In the prompt Select 13 option , prompt is as below:

```
(00)access-group      Specify access control for packets
(01)address           IP address
(02)beigrp           Enhanced Interior Gateway Routing Protocol
.....
```

Please Input the code of command to be excute(0-18): 1

input 1 , Select address option , prompt is as below:

```
(00)A.B.C.D          IP address
(01)dhcp             IP Address negotiated via DHCP
```

Please Input the code of command to be excute(0-1): 0

input 0 , Select A.B.C.D option , then prompt is as below:

Please input a IP Address:

input address , prompt is as below:

```
(00)A.B.C.D          IP netmask
```

Please Input the code of command to be excute(0-0): 0

input 0 , Select A.B.C.D option , then prompt is as below:

Please input a IP Address:

input mask , prompt is as below:

```
(00)secondary Make this IP address a secondary address
```

```
(01)<cr>
```

Please Input the code of command to be excute(0-1): 1

Select 1 , confirm it.

### 5.9.15 Configure the OSPF Administrative Distances

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer between 0 and 255. In general, the higher the value is, the lower the trust rating is. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

OSPF uses three different administrative distances: intra-area, inter-area, and external. Routes within an area are intra-area; routes to another area are inter-area; and routes from another routing domain learned via redistribution are external. The default distance for each type of route is 110.

To change any of the OSPF distance values, use the following command in router configuration mode:

Command	Purpose
<b>distance ospf [intra-area <i>dist1</i>] [inter-area <i>dist2</i>] [external <i>dist3</i>]</b>	Change the OSPF distance values of intra-area, inter-area and external route.

In the prompt select 6 option , prompt is as below:

```
(00)<1-255>          Set distance
```

```
(01)ospf             OSPF distance
```

Please Input the code of command to be excute(0-1): 1

input 1 , Select ospf option , prompt is as below:

```
(00)external          External type 5 and 7 routes
```

```
(01)inter-area        Inter-area routes
```

```
(02)intra-area        Intra-area routes
```

Please Input the code of command to be excute(0-2): 0

Select parameter and specify the administrative distance value .

### 5.9.16 Configure Route Calculation Timers

You can configure the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation. You can also configure the hold time between two consecutive SPF calculations. To do this, use the following command in router configuration mode:

Command	Purpose
<b>timers delay</b> <i>delaytime</i>	Set a timer delay of route calculation in an area.
<b>timers hold</b> <i>holdtime</i>	Set a minimum timer interval of route calculation in an area.

在 promptselect 21 option , prompt is as below:

```
(00)delay          Delay between receiving a change to SPF calculation
(01)hold          Hold time between consecutive SPF calculations
Please Input the code of command to be excute(0-1): 0
Select 0 , then specify the time delay for route calculating.
Select 1 , then configure the minimum interval of route calculating.
```

### 5.9.17 Monitor and Maintain OSPF

You can display specific statistics such as the contents of IP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path your device's packets are taking through the network.

To display various routing statistics, use the following commands:

Display general information about OSPF routing processes:

```
show ip ospf [process-id]
```

Display lists of information related to the OSPF database:

```
show ip ospf [process-id] database
```

```
show ip ospf [process-id] database [router] [link-state-id]
```

```
show ip ospf [process-id] database [router] [self-originate]
```

```
show ip ospf [process-id] database [router] [adv-router [ip-address]]
```

```
show ip ospf [process-id] database [network] [link-state-id]
```

```
show ip ospf [process-id] database [summary] [link-state-id]
```

```
show ip ospf [process-id] database [asbr-summary] [link-state-id]
```

```
show ip ospf [process-id] database [external] [link-state-id]
```

```
show ip ospf [process-id] database [database-summary]
```

Display the internal OSPF routing table entries to Area Border Router (ABR) and Autonomous System Boundary

Router (ASBR):

```
show ip ospf border-routers
```

Display OSPF-related interface information:

```
show ip ospf interface
```

Display OSPF-neighbor information on a per-interface basis:

```
show ip ospf neighbor
```

Monitor the process of establish OSPF neighbor:

```
debug ip ospf adj
```

Monitor the event of OSPF neighbor and interface:

```
debug ip ospf events
```

Monitor the process of OSPF database extending:

**debug ip ospf flood**

Monitor the process of OSPF LSA generating:

**debug ip ospf lsa-generation**

Monitor OSPF message:

**debug ip ospf packet**

Monitor the process of OSPF message retransmitting:

**debug ip ospf retransmission**

Monitor OSPF SPF calculating route:

**debug ip ospf spf**

**debug ip ospf spf intra**

**debug ip ospf spf inter**

**debug ip ospf spf external**

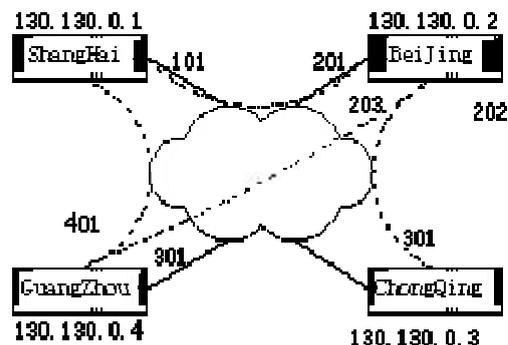
Monitor the establishing of OSPF SPF tree:

**debug ip ospf tree**

### 5.9.18 OSPF Configuration Examples

#### OSPF Point-to-Multipoint Example

BEIJING uses DLCI 201 to communicate with SHANGHAI, DLCI 202 to CHONGQING, and DLCI 203 to GUANGZHOU. SHANGHAI uses DLCI 101 to communicate with BEIJING and DLCI 102 to communicate with GUANGZHOU. GUANGZHOU communicates with SHANGHAI (DLCI 401) and BEIJING (DLCI 402). CHONGQING communicates with BEIJING (DLCI 301).



BEIJING Configuration:

```
hostname Beijing
```

```
!
```

```
interface serial 1/0
```

```
ip address 130.130.0.2 255.255.0.0
```

```
encapsulation frame-relay
```

```
frame-relay map 130.130.0.1 pvc 201 broadcast
```

```
frame-relay map 130.130.0.3 pvc 202 broadcast
```

```
frame-relay map 130.130.0.4 pvc 203 broadcast
```

```
ip ospf network point-to-multipoint
```

```
!
```

```
router ospf 1
```

```
network 130.130.0.0 255.255.0.0 area 0
```

ShangHai Configuration:

```
hostname shanghai
```

```
!
```

```
interface serial 1/0
```

```
ip address 130.130.0.1 255.0.0.0
encapsulation frame-relay
frame-relay map 130.130.0.2 pvc 101 broadcast
frame-relay map 130.130.0.4 pvc 102 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
GuangZhou Configuration:
hostname guangzhou
!
interface serial 1/0
ip address 130.130.0.4 255.0.0.0
encapsulation frame-relay
physical speed 1000000
frame-relay map 130.130.0.1 pvc 401 broadcast
frame-relay map 130.130.0.2 pvc 402 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
ChongQing Configuration:
hostname chongqing
!
interface serial 1/1
ip address 130.130.0.3 255.0.0.0
encapsulation frame-relay
physical speed 2000000
frame-relay map 130.130.0.2 pvc 301 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
```

### **OSPF Point-to-Multipoint, Nonbroadcast Example**

```
interface Serial1/0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
frame-relay local-dlci 200
frame-relay map 10.0.1.3 pvc 202
frame-relay map 10.0.1.4 pvc 203
frame-relay map 10.0.1.5 pvc 204
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
```

```
neighbor 10.0.1.5 cost 15
```

The following example is the configuration for the router on the other side:

```
interface Serial1/2
 ip address 10.0.1.3 255.255.255.0
 encapsulation frame-relay
 ip ospf network point-to-multipoint non-broadcast
 no ip mroute-cache
 no keepalive
 no fair-queue
 frame-relay local-dlci 301
 frame-relay map 10.0.1.1 pvc 300
 no shut
 !
 router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
```

### Variable-Length Subnet Masks Example

OSPF, static routes, and IS-IS support variable-length subnet masks (VLSMs). With VLSMs, you can use different masks for the same network number on different interfaces, which allows you to conserve IP addresses and more efficiently use available address space.

In the following example, a 30-bit subnet mask is used, leaving two bits of address space reserved for serial line host addresses. There is sufficient host address space for two host endpoints on a point-to-point serial link.

```
interface ethernet 1/0
 ip address 131.107.1.1 255.255.255.0
 ! 8 bits of host address space reserved for ethernet
interface serial 1/1
 ip address 131.107.254.1 255.255.255.252
 ! 2 bits of address space reserved for serial lines
 ! Router is configured for OSPF and assigned AS 107
router ospf 107
 ! Specifies network directly connected to the router
 network 131.107.0.0 0.0.255.255 area 0.0.0.0
```

### OSPF Routing and Route Redistribution Examples

#### OSPF Routing and Route Redistribution Examples

OSPF typically requires coordination among many internal routers, area border routers, and autonomous system boundary routers. At a minimum, OSPF-based routers can be configured with all default parameter values, with no authentication, and with interfaces assigned to areas.

Three examples follow:

1. The first is a simple configuration illustrating basic OSPF commands.
2. The second example illustrates a configuration for an internal router, ABR, and ASBRs within a single, arbitrarily assigned, OSPF autonomous system.
3. The third example illustrates a more complex configuration and the application of various tools available for controlling OSPF-based routing environments.

#### Basic OSPF Configuration Example

The following example illustrates a simple OSPF configuration that enables OSPF routing process 9000, attaches Ethernet 0 to area 0.0.0.0, and redistributes RIP into OSPF, and OSPF into RIP:

```
interface ethernet 1/0
  ip address 130.130.1.1 255.255.255.0
  ip ospf cost 1
!
interface ethernet 1/0
  ip address 130.130.1.1 255.255.255.0
!
router ospf 90
  network 130.130.0.0 255.255.0.0 area 0
  redistribute rip
!
router rip
  network 130.130.0.0
  redistribute ospf 90
```

### Basic OSPF Configuration Example for Internal Router, ABR, and ASBRs

The following example illustrates the assignment of four area IDs to four IP address ranges. In the example, OSPF routing process 109 is initialized, and four OSPF areas are defined: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, while Area 0 enables OSPF for all other networks.

```
router ospf 109
  network 131.108.20.0 255.255.255.0 area 10.9.50.0
  network 131.108.0.0 255.255.0.0 area 2
  network 131.109.10.0 255.255.255.0 area 3
  network 0.0.0.0 0.0.0.0 area 0
!
! Interface Ethernet1/0 is in area 10.9.50.0:
interface ethernet 1/0
  ip address 131.108.20.5 255.255.255.0
!
! Interface Ethernet1/1 is in area 2:
interface ethernet 1/1
  ip address 131.108.1.5 255.255.255.0
!
! Interface Ethernet1/2 is in area 2:
interface ethernet 1/2
  ip address 131.108.2.5 255.255.255.0
!
! Interface Ethernet1/3 is in area 3:
interface ethernet 1/3
  ip address 131.109.10.5 255.255.255.0
!
! Interface Ethernet1/4 is in area 0:
interface ethernet 1/4
  ip address 131.109.1.1 255.255.255.0
!
! Interface FastEthernet0/0 is in area 0:
```

```
interface FastEthernet0/0
  ip address 10.1.0.1 255.255.0.0
```

Each **network area** router configuration command is evaluated sequentially, so the order of these commands in the configuration is important. The D-Link router sequentially evaluates the *address/wildcard-mask* pair for each interface. See the "OSPF Commands" chapter of the *Network Protocols Command Reference* for more information.

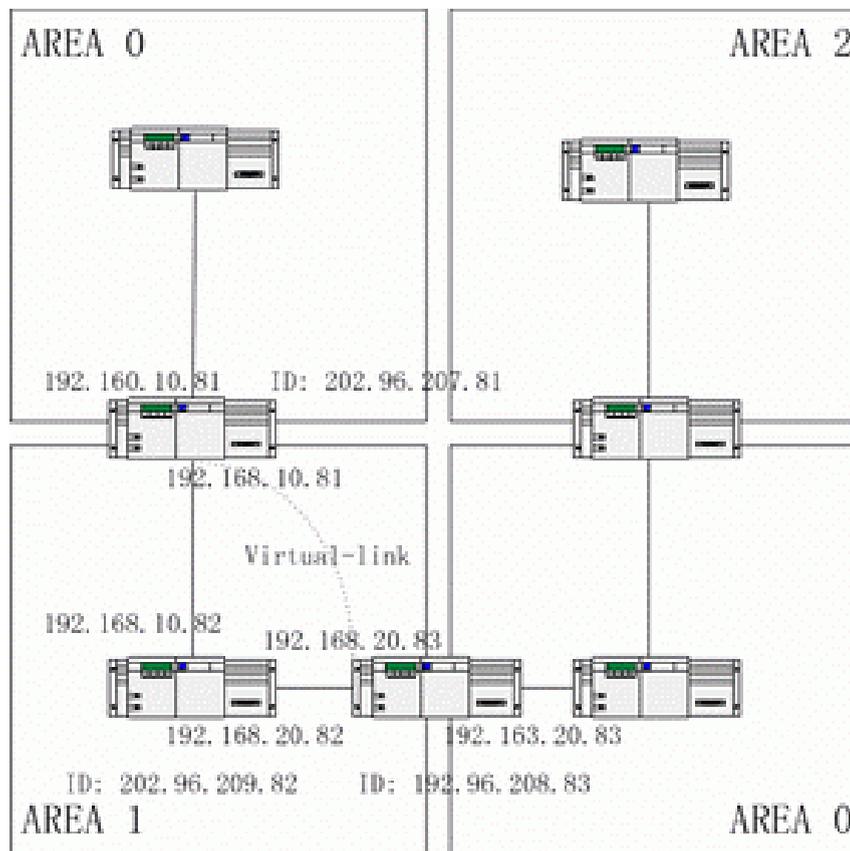
Consider the first **network area** command. Area ID 10.9.50.0 is configured for the interface on which subnet 131.108.20.0 is located. Assume that a match is determined for interface Ethernet 0. Interface Ethernet 0 is attached to Area 10.9.50.0 only.

The second **network area** command is evaluated next. For Area 2, the same process is then applied to all interfaces (except interface Ethernet 0). Assume that a match is determined for interface Ethernet 1. OSPF is then enabled for that interface and Ethernet 1 is attached to Area 2.

This process of attaching interfaces to OSPF areas continues for all **network area** commands. Note that the last **network area** command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to Area 0.

### Complex Internal Router, ABR, and ASBRs Example

The following example outlines a configuration for several routers within a single OSPF autonomous system. Figure 24 provides a general network map that illustrates this example configuration.



Configure router according to Figure 28 above

Router A:

```
interface loopback 0/0
  ip address 202.96.207.81 255.255.255.0
!
interface Ethernet 1/0
  ip address 192.168.10.81 255.255.255.0
!
interface ethernet 1/0
  ip address 192.160.10.81 255.255.255.0
```

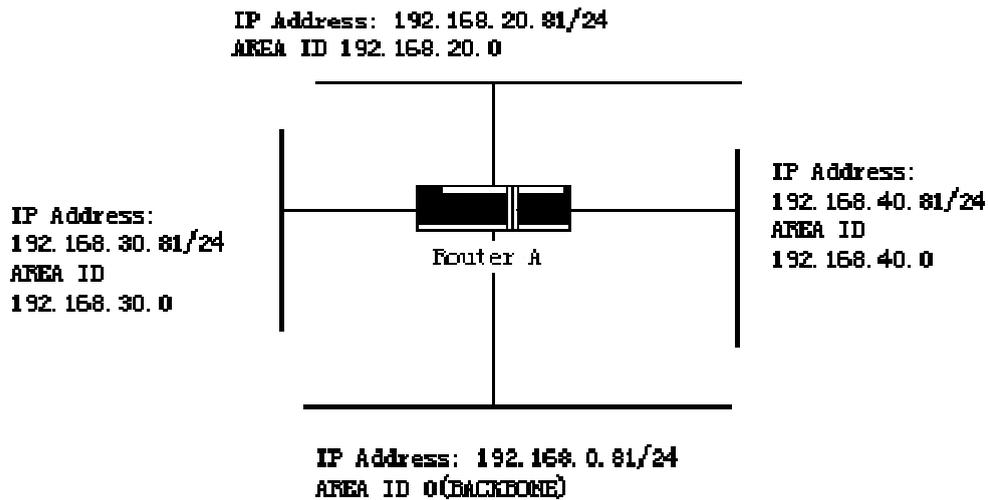
```
!  
router ospf 192  
  network 192.168.10.0 255.255.255.0 area 1  
  network 192.160.10.0 255.255.255.0 area 0  
!  
Router B:  
interface loopback 0/0  
  ip address 202.96.209.82 255.255.255.252  
!  
interface Ethernet 1/0  
  ip address 192.168.10.82 255.255.255.0  
!  
interface ethernet 1/1  
  ip address 192.160.20.82 255.255.255.0  
!  
router ospf 192  
  network 192.168.20.0 255.255.255.0 area 1  
  network 192.168.10.0 255.255.255.0 area 1  
!  
Router C:  
interface loopback 0/0  
  ip address 202.96.208.83 255.255.255.252  
!  
interface Ethernet 1/0  
  ip address 192.163.20.83 255.255.255.0  
!  
interface ethernet 1/1  
  ip address 192.160.20.83 255.255.255.0  
!  
router ospf 192  
  network 192.168.20.0 255.255.255.0 area 1  
  network 192.163.20.0 255.255.255.0 area 0  
!
```

### **Complex OSPF Configuration for ABR Examples**

The following example configuration accomplishes several tasks in setting up an ABR. These tasks can be split into two general categories:

1. Basic OSPF configuration
2. Route redistribution

The specific tasks outlined in this configuration are detailed briefly in the following descriptions. Figure 25 illustrates the network address ranges and area assignments for the interfaces.



The basic configuration tasks in this example are as follows:

1. Configure address ranges for Ethernet 0 through Ethernet 3 interfaces.
2. Enable OSPF on each interface.
3. Set up an OSPF authentication password for each area and network.
4. Assign link state metrics and other OSPF interface configuration options.
5. Create a stub area with area id 36.0.0.0. (Note that the authentication and stub options of the area router configuration command are specified with separate area command entries, but can be merged into a single area command.)
6. Specify the backbone area (Area 0).

Configuration tasks associated with redistribution are as follows:

1. Redistribute IGRP and RIP into OSPF with various options set (including metric-type, metric, tag, and subnet).
2. Redistribute IGRP and OSPF into RIP.

The following is an example OSPF configuration:

```
interface ethernet 1/0
  ip address 192.168.20.81 255.255.255.0
  ip ospf password GHGHGHG
  ip ospf cost 10
!
interface ethernet 1/1
  ip address 192.168.30.81 255.255.255.0
  ip ospf password ijklmnop
  ip ospf cost 20
  ip ospf retransmit-interval 10
  ip ospf transmit-delay 2
  ip ospf priority 4
!
interface ethernet 1/2
  ip address 192.168.40.81 255.255.255.0
  ip ospf password abcdefgh
  ip ospf cost 10
!
```

```
interface ethernet 1/3
  ip address 192.168.0.81 255.255.255.0
  ip ospf password ijklmnop
  ip ospf cost 20
  ip ospf dead-interval 80
!
router ospf 192
  network 192.168.0.0 255.255.255.0 area 0
  network 192.168.20.0 255.255.255.0 area 192.168.20.0
  network 192.168.30.0 255.255.255.0 area 192.168.30.0
  network 192.168.40.0 255.255.255.0 area 192.168.40.0
  area 0 authentication simple
  area 192.168.20.0 stub
  area 192.168.20.0 authentication simple
  area 192.168.20.0 default-cost 20
  area 192.168.20.0 authentication simple
  area 192.168.20.0 range 36.0.0.0 255.0.0.0
  area 192.168.30.0 range 192.42.110.0 255.255.255.0
  area 0 range 130.0.0.0 255.0.0.0
  area 0 range 141.0.0.0 255.0.0.0
  redistribute rip

  RIP on network 192.168.30.0
  router rip
    network 192.168.30.0
    redistribute ospf 192
  !
```

## 5.10 Configure BGP Task List

### 5.10.1 BGP Overview

This chapter describes how to configure Border Gateway Protocol (BGP). For a complete description of the BGP commands in this chapter, refer to the "BGP Commands" chapter.

The Border Gateway Protocol, as defined in RFCs 1163, 1267 and 1771, is an Exterior Gateway Protocol (EGP). It allows you to set up an interdomain routing system that provides the loop-free exchange of routing information between autonomous systems. This section will describe following contents:

### 5.10.2 D-Link BGP Implementation

In BGP, each route consists of a reachable destination (network or prefix), a list of autonomous systems that information has passed through (called the autonomous system path), and a list of other path attributes. D-Link supports RFC1771 defined BGP Versions 4.

The primary function of a BGP system is to exchange network reachability information with other BGP systems, including information about the list of autonomous system paths. This information can be used to construct a graph of autonomous system connectivity from which routing loops can be pruned and with which autonomous system-level policy decisions can be enforced. BGP Version 4 supports classless interdomain routing (CIDR), which lets you reduce the size of your routing tables by creating aggregate routes, resulting in supernets. CIDR eliminates the concept of network classes within BGP and supports the advertising of IP prefixes. CIDR routes can be carried by Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), and Intermediate System-to-Intermediate System (ISIS)-IP, and Routing Information Protocol Version 2(RIP2).

The external gateway route provides better control capability than internal gateway route. It is also the main distinguish of external and internal gateway route. The BGP implementation offers multiple optional methods for the route control:

- To filter route, you can use access-list, aspath-list and prefix-list based on neighbor, you can also use access-list and prefix-list based on port.
- To change the route attribute, you can use route-map to change the BGP route attributes, such as MED, Local Preference, weight, etc.
- To communicate with interior dynamic routing protocol (OSPF, RIP, etc), you can use redistribute to automatically generate the BGP routing information. You can also manually configure network and aggregate to generate the BGP route. At the time of generating BGP route, you can configure the route attribute with route-map.
- To control the priority of a BGP route in the system, you can configure the administrative distance of the BGP route with the command distance.

### How BGP Select s Paths

BGP bases its decision process on the attribute values. When faced with multiple routes to the same destination, BGP chooses the best route for routing traffic toward the destination. The following process summarizes how BGP chooses the best route:

1. If the next hop is inaccessible, do not consider it.
2. If the path is internal, synchronization is enabled, and the route is not in the IGP, do not consider the route.
3. Prefer the path with the largest weight (weight is a D-Link proprietary parameter).
4. If the routes have the same weight, prefer the route with the largest local preference.
5. If the routes have the same local preference, prefer the route that was originated by the local router. For example, a route might be originated by the local router using the network bgp router configuration command, or through redistribution from an IGP.
6. If the local preference is the same, or if no route was originated by the local router, prefer the route with the shortest autonomous system path.
7. If the autonomous system path length is the same, prefer the route with the lowest origin code (IGP < EGP < INCOMPLETE).
8. If the origin codes are the same, prefer the route with the lowest MED metric attribute.
9. If the routes have the same MED, prefer EBGp instead of IBGP. All routes in AS federation is considered as interior routes, but router will prefer federal EBGp instead of IBGP.
10. Prefer the route with the lowest IP address value for the BGP router ID if each route has the same connecting attribution.

### Basic BGP Configuration Tasks

The BGP configuration tasks are divided into basic and advanced tasks. The first two basic tasks are required to configure BGP; the remaining basic and advanced tasks are optional.

Basic BGP configuration tasks in the following sections:

- [Enable BGP Routing Selection](#)
- [Configure BGP Neighbors](#)
- [Configure BGP Soft Reconfiguration](#)
- [Reset BGP Connections](#)
- [Configure BGP Interactions with IGPs](#)
- [Configuring BGP Route Cost](#)
- [Configure BGP Route Filtering base on Neighbor](#)
- [Configure BGP Route Filtering base on Port](#)
- [Disable Next-Hop Processing on BGP Updates](#)

### Advanced BGP Configuration Tasks

Advanced, optional BGP configuration tasks are discussed in the following sections:

- [Use Route Maps Filtering and Modify Route Updates](#)
- [Configure Aggregate Addresses](#)
- [Configure BGP Community Property](#)

- [Configuring Self-Administration System Confederation](#)
- [Configuring a Route Reflector](#)
- [Disabling Peer Group](#)
- [Configure Multi-Hop Exterior Peer Groups](#)
- [Setting BGP Route Administrative Distance](#)
- [Adjusting BGP Timers](#)
- [Compare the MEDs from Different Autonomous Systems Route](#)

For information on configuring features that apply to multiple IP routing protocols (such as redistributing routing information), see the chapter "Configuring IP Routing Protocol-Independent Features."

### Configuring Basic BGP Features

The tasks described in this section are for configuring basic BGP features.

- [Enabling BGP Routing Select ion](#)
- [Configure BGP Neighbors](#)
- [Configure BGP Soft Reconfiguration](#)
- [Reset BGP Connections](#)
- [Configure BGP Interactions with IGP](#)
- [Configuring BGP Weights](#)
- [Configure BGP Route Filtering by Neighbor](#)
- [Configure BGP Route Filtering base on Port](#)
- [Disable Next-Hop Processing on BGP Updates](#)

### Enable BGP Routing Select ion

To enable BGP routing select ion, using the following commands beginning in global configuration mode:

Step	Command	Purpose
1.	<b>router bgp</b> <i>autonomous-system</i>	Enable a BGP routing process, which places you in router configuration mode. Flag a network as local to this autonomous system and enter it to the BGP table.
2.	<b>network</b> <i>network-number/masklen</i> [ <i>route-map route-map-name</i> ]	

Step1 :

input routerCommand ,prompt is as below:

- ```
(00)beigrp      Enable BEIGRP (compatible with eigrp)
(01)bgp        Enable Border Gateway Protocol (BGP)
(02)ospf       Enable Open Shortest Path First (OSPF)
(03)rip        Enable Routing Information Protocol(RIP)
```

Please Input the code of command to be excute(0-3): 1

input 1 ,Select bgp option ,prompt is as below:

```
(00)<1-65535>      Local anonymous system number
```

Please Input the code of command to be excute(0-0): 0

input 0 ,then prompt is as below:

Please input a digital number:Please input a string:

input autonomous-system value .

Step2 :

In the prompt Select 13 option ,prompt is as below:

```
(00)A.B.C.D/n      IP Prefix
```

Please Input the code of command to be excute(0-0): 0

input 0 ,prompt is as below:

Please input a string:

input network-number/masklen value ,prompt is as below:

```
(00)backdoor          Specify a BGP backdoor route
(01)route-map         Route map to modify the attribute
(02)<cr>
Please Input the code of command to be excute(0-2):
Select detailed parameter .
```

Note: For exterior protocols, a reference to an IP network from the network router configuration command controls only which networks are advertised. This behavior is in contrast to IGP, such as IGRP, which also use the network command to determine where to send updates.

**Note:** The network command **network** is used to inject IGP routes into the BGP table. The resources of the router, such as configured NVRAM or RAM, determine the upper limit of the number of network commands you can use. Alternatively, you could use the redistribute router configuration command **redistribute** to achieve the same result.

### 5.10.3 Configure BGP Neighbors

The purpose of BGP configuration is establishing the project of exchange route information. BGP must be configured neighbors for exchange the route information with outside.

BGP supports two kinds of neighbors: internal and external. Internal neighbors are in the same autonomous system; external neighbors are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors may be anywhere in the same autonomous system.

To configure BGP neighbors, use the following command in router configuration mode:

| Command                                                                | Purpose                   |
|------------------------------------------------------------------------|---------------------------|
| <b>neighbor</b> {ip-address   peer-group-name} <b>remote-as</b> number | Specifies a BGP neighbor. |

In the prompt Select 12 option ,prompt is as below:

```
(00)A.B.C.D          IP address of neighbor
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option , prompt is as below:
Please input a IP Address:
input IP , then prompt is as below:
(00)default-originate      Permit announcement of default route to neighbor
.....
(08)remote-as             Specify a BGP neighbor's AS
.....
Please Input the code of command to be excute(0-17): 8
input 8 , Select remote-as option , prompt is as below:
(00)<1-65535>           Autonomous system number of remote neighbor
Please Input the code of command to be excute(0-0): 0
input 0 , prompt is as below:
Please input a digital number:Please input a string:
input number value , prompt is as below:
(00)passive             Set the neighbor to passive
(01)<cr>
```

Please Input the code of command to be excute(0-1): 1  
Select 1 and confirm it.

See the "BGP Neighbor Configuration Examples" section at the end of this chapter for an example of configuring BGP neighbors.

### 5.10.4 Configure BGP Soft Reconfiguration

Normally, BGP neighbor only exchanges all the routes while establishing the connection, after that only the variable route can be exchanged. Whenever there is a change in the policy, the BGP session has to be cleared for the new policy to take effect. Clearing a BGP session causes cache invalidation and results in a tremendous impact on the operation of networks. Soft reconfiguration allows policies to be configured and activated without clearing the BGP session. Soft reconfiguration is recommended; it is done on a per-neighbor basis. When soft reconfiguration is used to generate inbound updates from a neighbor, it is called inbound soft reconfiguration. When soft reconfiguration is used to send a new set of updates to a neighbor, it is called outbound soft reconfiguration. Performing inbound reconfiguration enables the new inbound policy to take effect. Performing outbound reconfiguration causes the new local outbound policy take effect without resetting the BGP session. As a new set of updates is sent during outbound policy reconfiguration, a new inbound policy of the neighbor can also take effect.

In order to generate new inbound updates without resetting the BGP session, the local BGP speaker should store all the received updates without modification, regardless of whether it is accepted or denied by the current inbound policy. This is memory intensive and should be avoided. On the other hand, outbound soft reconfiguration does not have any memory overhead. One could trigger an outbound reconfiguration in the other side of the BGP session to make the new inbound policy take effect.

To allow inbound reconfiguration, BGP should be configured to store all received updates. Outbound reconfiguration does not require preconfiguration.

To configure BGP soft configuration, use the following command in router configuration mode:

| Command                                                                        | Purpose                             |
|--------------------------------------------------------------------------------|-------------------------------------|
| <b>Neighbor</b> {ip-address peer-group-name} soft-reconfiguration<br>[inbound] | Configure BGP soft reconfiguration. |

In the prompt Select 12 option ,prompt is as below:

```
(00)A.B.C.D      IP address of neighbor
Please Input the code of command to be excute(0-0): 0
input 0 ,Select A.B.C.D option , prompt is as below:
Please input a IP Address:
input IP , then prompt is as below:
(00)default-originate      Permit announcement of default route to neighbor
.....
(14)soft-reconfiguration   Enable soft reconfiguration
.....
Please Input the code of command to be excute(0-17): 14
input 14 ,Select remote-as option , prompt is as below:
(00)inbound      Store inbound announcement from neighbor
Please Input the code of command to be excute(0-0): 0
input 0 , Select inbound option .
```

If you specify a BGP peer group by using the peer-group-name argument, all members of the peer group will inherit the characteristic configured with this command.

### 5.10.5 Reset BGP Connections

Once you have defined two routers to be BGP neighbors, they will form a BGP connection and exchange routing information. If you subsequently change a BGP filter, weight, distance, version, or timer, or make a similar configuration change, you must reset BGP connections for the configuration change to take effect. Use either of the following

commands in EXEC mode to reset BGP connections:

| Command                     | Purpose                            |
|-----------------------------|------------------------------------|
| <b>clear ip bgp *</b>       | Reset all BGP connections.         |
| <b>clear ip bgp address</b> | Reset a particular BGP connection. |

Take the first command for an example. :

input clear Command , prompt is as below:

```
(00)arp-cache          Clear the entire ARP cache
(01)dialer             Clear dialer statistics
(02)frame-relay-inarp  Clear inverse ARP entries from the map table
(03)ip                IP
.....
```

Please Input the code of command to be excute(0-11): 3

input 3 , Select ip option , prompt is as below:

```
(00)beigrp           Clear BEIGRP
(01)bgp              BGP information
(02)dhcpcd           DHCP Server information
.....
```

Please Input the code of command to be excute(0-5): 1

input 1 , Select bgp option , then prompt is as below:

```
(00)*                Clear all peers
(01)<1-65535>         Clear peers by specified AS number
(02)A.B.C.D          IP address of neighbor to clear
.....
```

Please Input the code of command to be excute(0-7): 0

input 0 , Select all option , prompt is as below:

```
(00)soft Soft reconfigure
(01)<cr>
```

Please Input the code of command to be excute(0-1): 1

input 1 and confirm it.

### 5.10.6 Configure synchronization between BGP and IGP

If your autonomous system will be passing traffic through it from another autonomous system to a third autonomous system, it is very important that your autonomous system be consistent about the routes that it advertises. For example, if your BGP were to advertise a route before all routers in your network had learned about the route through your IGP, your autonomous system could receive traffic that some routers cannot yet route. To prevent this from happening, BGP must wait until the IGP has propagated routing information across your autonomous system. This causes BGP to be synchronized with the IGP. Synchronization is enabled by default.

In some cases, you do not need synchronization. If you will not be passing traffic from a different autonomous system through your autonomous system, or if all routers in your autonomous system will be running BGP, you can disable synchronization. Disabling this feature can allow you to carry fewer routes in your IGP and allow BGP to converge more quickly. To disable synchronization, use the following command in router configuration mode:

| Command                       | Purpose                                         |
|-------------------------------|-------------------------------------------------|
| <b>Synchronization (undo)</b> | Disable synchronization between BGP and an IGP. |

在路由 prompt 中，先 Select U or u，prompt is as below:

```
(00)aggregate-address          Aggregate network
.....
(22)synchronization          Perform IGP synchronization
.....
```

Please Input the code of command to be excute(0-26): 22

input 22，Select synchronization option，prompt is as below:

```
(00)<cr>
```

Please Input the code of command to be excute(0-0): 0

input 0，confirm it.

When you disable synchronization, you should also clear BGP sessions using the clear ip bgp command.

See the "BGP Path Filtering by Neighbor Example" section at the end of this chapter for an example of BGP synchronization.

In general, you will not want to redistribute most BGP routes into your IGP. A common design is to redistribute one or two routes and to make them exterior routes in IGRP, or have your BGP speaker generate a default route for your autonomous system. When redistributing from BGP into IGP, only the routes learned using EBGP get redistributed. In most circumstances, you also will not want to redistribute your IGP into BGP. Just list the networks in your autonomous system with network router configuration commands and your networks will be advertised. Networks that are listed this way are referred to as local networks and have a BGP origin attribute of "IGP." They must appear in the main IP routing table and can have any source; for example, they can be directly connected or learned via an IGP. The BGP routing process periodically scans the main IP routing table to detect the presence or absence of local networks, updating the BGP routing table as appropriate. If you do perform redistribution into BGP, you must be very careful about the routes that can be in your IGP, especially if the routes were redistributed from BGP into the IGP elsewhere. This creates a situation where BGP is potentially injecting information into the IGP and then sending such information back into BGP, and vice versa.

### 5.10.7 Configuring BGP Weights

An administrative weight is a number that you can assign to a path so that you can control the path selection process. The administrative weight is local to the router. A weight can be a number from 0 to 65535. Paths that the local software originates have weight 32768 by default; other paths have weight 0. Administrator can implement routing policy through changing administrative weights.

Perform the following task in router configuration mode to configure BGP administrative weights:

| Command                                                                    | Purpose                                          |
|----------------------------------------------------------------------------|--------------------------------------------------|
| <b>neighbor</b> <i>{ip-address / peer-group-name}</i> <i>weight weight</i> | Specify a weight for all routes from a neighbor. |

In the prompt Select 12 option，prompt is as below:

```
(00)A.B.C.D          IP address of neighbor
```

Please Input the code of command to be excute(0-0): 0

input 0，Select A.B.C.D option，prompt is as below:

Please input a IP Address:

input IP，then prompt is as below:

```
(00)default-originate      Permit announcement of default route to neighbor
.....
```

```
(17)weight                Default weight value
```

Please Input the code of command to be excute(0-17): **17**

input 17 , Select weight option , prompt is as below:

(00)<0-65535> Weight value

Please Input the code of command to be excute(0-0): **0**

input 0 , then prompt is as below:

Please input a digital number:Please input a string:

input weight.

In addition, you can assign weights through route-map.

### 5.10.8 Configure the BGP Route Filtering based on Neighbor

D-Link BGP implementation can specify the BGP routes with four kinks of filtering:

1. Use the global configuration command **ip aspath-list** and **neighbor filter-list** command together to apply the Aspath list filter.

| Step | Command                                                                                                                                                                               | Purpose                              |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 1.   | <b>ip aspath-list</b> <i>aspaths-list-name</i> { <b>permit</b>   <b>deny</b> }                                                                                                        | Define an access list about BGP.     |
| 2.   | <i>as-regular-expression</i>                                                                                                                                                          | Enter the router configuration mode. |
| 3.   | <b>router bgp</b> <i>autonomous-system</i><br><b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>filter-list</b><br><i>aspath-list-name</i> { <b>in</b>   <b>out</b> } | Set up a BGP filter.                 |

Step1 :

input **ip** Command , prompt is as below:

(00)access-list Named access-list

(01)as-path BGP as-path access list definition

(02)community-list Community attribute list definition

.....

Please Input the code of command to be excute(0-20): **1**

input 1 , Select as-path option , prompt is as below:

(00)access-list AS-Path access list

Please Input the code of command to be excute(0-0): **0**

input 0 , Select access-list option , prompt is as below:

(00)help Help information of aspath regular expression

(01)WORD Name of AS-path access list

Please Input the code of command to be excute(0-1): **1**

input 1 , Select WORD option , prompt is as below:

Please input a string:

input string , then prompt is as below:

(00)deny Access list for denies

(01)permit Access list for permits

Please Input the code of command to be excute(0-1):

Select parameter , and confirm itLINE value .

Step2 :

input **router** Command , prompt is as below:

(00)beigrp Enable BEIGRP (compatible with eigrp)

(01)bgp Enable Border Gateway Protocol (BGP)

(02)ospf Enable Open Shortest Path First (OSPF)

(03)rip Enable Routing Information Protocol(RIP)

Please Input the code of command to be excute(0-3): **1**

input 1 , Select bgp option , prompt is as below:  
 (00)<1-65535> Local anonymous system number  
 Please Input the code of command to be excute(0-0): 0  
 Select 0 , prompt is as below:  
 Please input a digital number:Please input a string:  
 input *autonomous-system* value .  
 Step3 :  
 In the prompt Select 12 option , prompt is as below:  
 (00)A.B.C.D IP address of neighbor  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select A.B.C.D option , then prompt 为 :  
 Please input a IP Address:  
 input IP , prompt is as below:  
 (00)default-originate Permit announcement of default route to neighbor  
 (01)description Description of the neighbor  
 (02)distribute-list Distribute list  
 (03)ebgp-multihop Allow EBGp neighbor not directly connected  
 (04)filter-list AS-path filter list  
 .....  
 Please Input the code of command to be excute(0-17): 4  
 input 4 , Select filter-list option , prompt is as below:  
 (00)WORD Name of as-path filter list  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select WORD option , prompt is as below:  
 Please input a string:  
 input string , prompt is as below:  
 (00)in Filter incoming routes  
 (01)out Filter outgoing routes  
 Please Input the code of command to be excute(0-1):  
 Select parameter .

2. Use the global configuration command **ip access-list** and **neighbor distribute-list** command together to apply the access list.

| Setp | Command                                                                                                                                     | Purpose                              |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 1.   | <b>ip access-list standard</b> <i>access-list-name</i>                                                                                      | Define an access list.               |
| 2.   | <b>router bgp</b> <i>autonomous-system</i>                                                                                                  | Enter the router configuration mode. |
| 3.   | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>distribute-list</b> <i>access-list-name</i> { <b>in</b>   <b>out</b> } | Set up a BGP filter.                 |

Step1 :  
 input **ip** Command , prompt is as below:  
 (00)access-list Named access-list  
 (01)as-path BGP as-path access list definition  
 (02)community-list Community attribute list definition  
 .....  
 Please Input the code of command to be excute(0-20): 0  
 input 1 , Select access-list option , prompt is as below:  
 (00)extended Extended Access List  
 (01)standard Standard Access List

Please Input the code of command to be excute(0-1): **1**

input 1 , Select standard option , prompt is as below:

(00)WORD Standard Access-list name

Please Input the code of command to be excute(0-0): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:D-Link

input string .

Step2 :

input **router**Command , prompt is as below:

(00)beigrp Enable BEIGRP (compatible with eigrp)

(01)bgp Enable Border Gateway Protocol (BGP)

(02)ospf Enable Open Shortest Path First (OSPF)

(03)rip Enable Routing Information Protocol(RIP)

Please Input the code of command to be excute(0-3): **1**

input 1 , Select bgp option , prompt is as below:

(00)<1-65535> Local anonymous system number

Please Input the code of command to be excute(0-0): **0**

Select 0 , prompt is as below:

Please input a digital number:Please input a string:

input *autonomous-system* value .

Step3 :

In the prompt Select 12 option , prompt is as below:

(00)A.B.C.D IP address of neighbor

Please Input the code of command to be excute(0-0): **0**

input 0 , Select A.B.C.D option , then prompt :

Please input a IP Address:

input IP , prompt is as below:

(00)default-originate Permit announcement of default route to neighbor

(01)description Description of the neighbor

(02)distribute-list Distribute list

(03)ebgp-multihop Allow EBGp neighbor not directly connected

(04)filter-list AS-path filter list

.....

Please Input the code of command to be excute(0-17): **2**

input 2 , Select distribute-list option , prompt is as below:

(00)WORD Name of distribute-list

Please Input the code of command to be excute(0-0): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:

input string , prompt is as below:

(00)in Filter incoming routes

(01)out Filter outgoing routes

Please Input the code of command to be excute(0-1):

Select parameter .

3.Use the global configuration command **ip prefix-list** and **neighbor prefix-list** command together to apply the prefix list.

| Step | Command                                                        | Purpose               |
|------|----------------------------------------------------------------|-----------------------|
| 1.   | <b>ip prefix-list</b> <i>prefixs-list-name</i> { <b>permit</b> | Define a prefix list. |

|    |                                                                       |                                                              |
|----|-----------------------------------------------------------------------|--------------------------------------------------------------|
| 2. | <b> deny } A.B.C.D/n ge x le y</b>                                    | Enter the router configuration mode.<br>Set up a BGP filter. |
| 3. | <b>router bgp <i>autonomous-system</i></b>                            |                                                              |
|    | <b>neighbor { <i>ip-address</i>   <i>peer-group-name</i> }</b>        |                                                              |
|    | <b>prefix-list <i>prefix-list-name</i> { <b>in</b>   <b>out</b> }</b> |                                                              |

## Step1 :

input **ip** Command , prompt is as below:

(00)access-list          Named access-list

.....

(14)prefix-list          Prefix list definition

.....

Please Input the code of command to be excute(0-20): **14**

input 14 , Select prefix-list option , prompt is as below:

(00)sequence-number          Enable use of prefix-list sequence number

(01)WORD                      Name of prefix list

Please Input the code of command to be excute(0-1): **1**

input 1 , Select WORD option , prompt is as below:

Please input a string:

input *prefixs-list-name*string , then prompt is as below:

(00)deny                      Prefix list for denies

(01)description              Description information

(02)permit                    Prefix list for permites

(03)seq                      Sequence number of prefix list

Please Input the code of command to be excute(0-3): **2**

Select parameter and confirm itge or le value .

Step2 :

input **router** Command , prompt is as below:

(00)beigrp                    Enable BEIGRP (compatible with eigrp)

(01)bgp                      Enable Border Gateway Protocol (BGP)

(02)ospf                      Enable Open Shortest Path First (OSPF)

(03)rip                      Enable Routing Information Protocol(RIP)

Please Input the code of command to be excute(0-3): **1**

input 1 , Select bgp option , prompt is as below:

(00)<1-65535>              Local anonymous system number

Please Input the code of command to be excute(0-0): **0**

Select 0 , prompt is as below:

Please input a digital number:Please input a string:

input *autonomous-system* value .

Step3 :

In the prompt Select 12 option , prompt is as below:

(00)A.B.C.D                  IP address of neighbor

Please Input the code of command to be excute(0-0): **0**

input 0 , Select A.B.C.D option , then prompt :

Please input a IP Address:

input IP , prompt is as below:

(00)default-originate          Permit announcement of default route to neighbor

.....

(07)prefix-list              Prefix list

.....

Please Input the code of command to be excute(0-17): **7**

input 2 , Select prefix-list option , prompt is as below:

(00)WORD           Name of prefix-list

Please Input the code of command to be excute(0-0): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:

input string , prompt is as below:

(00)in               Filter incoming routes

(01)out             Filter outgoing routes

Please Input the code of command to be excute(0-1):

Select parameter .

4. Use the global command **route-map** and command **neighbor route-map** together to apply router mapping.

With route map you can not only filter but also change the route attribute, which will be presented in the following chapter.

About the examples of route filtering based on neighbor, refer to the [“Examples of the BGP Route Filtering based on Neighbor”](#).

### 5.10.9 Configure the BGP Route Filtering based on Port

You can use the access list and the prefix list to configure the BGP route filtering based on port. You can filter the network ID of the route, and you can also filter the gateway address of the route. You can specify the option access-list to use the access list to filter the network ID of the route, specify the prefix-list option to use the prefix list to filter the network ID, and specify the gateway option to use the access list to filter the Nexthop attribute of the route. You can even synchronously filter the network ID and the Nexthop attribute of the route, but the access-list option can't be used along with the prefix-list option. Specify '\*', you can filter the routes on all ports.

To configure the BGP route based on port, perform the following configuration in BGP configuration mode:

| Command                                                                                                                           | Purpose                             |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| <b>filter interface { in   out } { access-list access-list-name } { prefix-list prefix-list-name } gateway access-list-name }</b> | Filter the BGP route based on port. |

In the prompt Select 8 option , prompt is as below:

(00)interface-name

(01)\*               All interface

Please Input the code of command to be excute(0-1): **0**

input 0 , Select interface-name option , prompt is as below:

Please input a interface name:

input port , then prompt is as below:

(00)in               Filter incoming routing updates

(01)out             Filter outgoing routing updates

Please Input the code of command to be excute(0-1):

Select port filter pattern , then prompt is as below:

(00)access-list       Filter routes by access-list

(01)gateway           Filter gateway by access-list

(02)prefix-list       Filter routes by prefix-list

Please Input the code of command to be excute(0-2):

Select parameter .

Prefer the [“Examples of the BGP Route Map based on Port”](#) for the examples of route filtering based on port.

### 5.10.10 Disable Next-Hop Processing on BGP Updates

You can configure the router to disable next-hop processing for BGP updates to a neighbor. This might be useful in nonmeshed networks such as Frame Relay or X.25, where BGP neighbors might not have direct access to all other neighbors on the same IP subnet. There are two ways to disable next-hop processing:

1. provide a BGP connecting local IP address to instead the next-hop address of outbound routes;
2. use a route map to specify that the next-hop address of the inbound routes or the outbound routes (refer to other chapters)

To disable next-hop processing and provide a specific address to be used instead of the next-hop address, use the following command in router configuration mode:

| Command                                                                       | Purpose                                            |
|-------------------------------------------------------------------------------|----------------------------------------------------|
| <b>neighbor</b> <i>{ip-address / peer-group-name}</i><br><b>next-hop-self</b> | disable next-hop processing of BGP neighbor update |

input **neighbor** Command , prompt is as below:

(00)A.B.C.D IP address of neighbor

Please Input the code of command to be excute(0-0): **0**

input 0 , Select A.B.C.D option , then promptis as below :

Please input a IP Address:

input IP , prompt is as below:

(00)default-originate Permit announcement of default route to neighbor

.....

(06)next-hop-self Set nexthop value to self

.....

Please Input the code of command to be excute(0-17): **6**

input 6 , Select next-hop-self option .

Configuring this command causes the current router to advertise itself as the next hop for the specified neighbor. Therefore, other BGP neighbors will forward to it packets for that address. This is useful in a nonmeshed environment, since you know that a path exists from the present router to that address. In a network broadcast ing environment, this is not useful, since it will result in unnecessary extra hops.

### 5.10.11 Configure Advanced BGP Features

The tasks in this section are for configuring advanced BGP features.

#### Use Route Maps to Filter and Modify Route Updates

You can use a route map on a per-neighbor basis to filter updates and modify various attributes. A route map can be applied to either inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

On both the inbound and the outbound updates, we support matching based on autonomous system path, community, and network numbers. Autonomous system path matching requires the **aspath-list** command, community based matching requires the **community-list** command and network-based matching requires the **ip access-list** command.

Use the following BGP configuring command to configure the route update, which is modified and filtered by route map:

| Command                                                                                                                         | Purpose                                          |
|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| <b>neighbor</b> <i>{ip-address/peer-group-name}</i> <b>route-map</b><br><i>config-route-map-name</i> { <b>in</b>   <b>out</b> } | Apply a route map to inbound or outbound routes. |

In the prompt Select 12 option , prompt is as below:

(00)A.B.C.D                    IP address of neighbor  
Please Input the code of command to be excute(0-0): **0**  
input 0 , Select A.B.C.D option , then prompt :  
Please input a IP Address:  
input IP , prompt is as below:  
(00)default-originate            Permit announcement of default route to neighbor  
.....  
(09)route-map                    Apply route map to the neighbor  
.....  
Please Input the code of command to be excute(0-17): **9**  
input 9 , Select route-map option , prompt is as below:  
(00)WORD                        Name of route-map  
Please Input the code of command to be excute(0-0): **0**  
input 0 , Select WORD option , prompt is as below:  
Please input a string:  
input string , then prompt is as below:  
(00)in                            Map incoming routes  
(01)out                            Map outgoing routes  
Please Input the code of command to be excute(0-1):  
Select parameter .

See the "BGP Route Map Examples" section at the end of this chapter for BGP route-map examples.

### Configure Aggregate Addresses

Classless interdomain routing (CIDR) enables you to create aggregate routes (or supernets) to minimize the size of routing tables. You can configure aggregate routes in BGP either by redistributing an aggregate route into BGP or by using the conditional aggregation feature described in the following task table. An aggregate address will be added to the BGP table if there is at least one more specific entry in the BGP table.

To create an aggregate address in the routing table, use one or more of the following commands in router configuration mode:

| Command                                                       | Purpose                                                               |
|---------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>aggregate</b> <i>network/len</i>                           | Create an aggregate address in the BGP routing table.                 |
| <b>aggregate</b> <i>network/len summary-only</i>              | Advertise summary addresses only.                                     |
| <b>aggregate</b> <i>network/len config-route-map map-name</i> | Generate an aggregate based on conditions specified by the route map. |

Take the first command for an example. :

In the prompt Select 0 option , prompt is as below:  
(00)A.B.C.D/n                    IP Prefix  
Please Input the code of command to be excute(0-0): **0**  
input 0 , Select A.B.C.D option , prompt is as below:  
Please input a string:  
input network/len value , then prompt is as below:  
(00)route-map Route map to modify route attribute  
(01)summary-only Suppress more specific routes from announcement  
(02)<cr>  
Please Input the code of command to be excute(0-2):  
Select parameter .

See the "[BGP Aggregate Route Example](#)" section at the end of this chapter for examples of using BGP aggregate routes.

### Configure BGP Community Property

BGP supports transit policies via controlled distribution of routing information. The distribution of routing information is based on one of the following three values:

1. IP address (see the "Configure BGP Route Filtering by Neighbor" section earlier in this chapter).
2. The value of the AS\_PATH attribute (see the "Configure BGP Path Filtering by Neighbor" section earlier in this chapter).
3. The value of the COMMUNITIES attribute (as described in this section).

The COMMUNITIES attribute is a way to group destinations into communities and apply routing decisions based on the communities. This method simplifies a BGP speaker's configuration that controls distribution of routing information.

A community is a group of destinations that share some common attribute. Each destination can belong to multiple communities. Autonomous system administrators can define to which communities a destination belongs.

The COMMUNITIES attribute is an optional, transitive, global attribute in the numerical range from 1 to 4,294,967,200. Along with Internet community, there are a few predefined, well-known communities, as follows:

**no-export---** Do not advertise this route to EBGp peers(included EBGp peers of internal autonomous system).

**no-advertise---** Do not advertise this route to any peer.

**local-as---** Do not advertise this route to peers outside the autonomous system (can be advertised to other sub-autonomous systems).

A BGP speaker can set, append, or modify the community of a route when you generate, receive or retransmit routes. When routes are aggregated, the resulting aggregate has a COMMUNITIES attribute that contains all communities from all the initial routes.

By default, no COMMUNITIES attribute is sent to a neighbor. You can specify that the COMMUNITIES attribute be sent to the neighbor by using the following command in router configuration mode:

| Command                                                | Purpose                                                   |
|--------------------------------------------------------|-----------------------------------------------------------|
| neighbor {ip-address   peer-group-name} send-community | Specify that the COMMUNITY attribute be sent to neighbor. |

In the prompt Select 12 option , prompt is as below:

```
(00)A.B.C.D      IP address of neighbor
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option , then prompt 为 :
Please input a IP Address:
input IP ,prompt is as below:
(00)default-originate      Permit announcement of default route to neighbor
.....
(12)send-community        Allow send community attribute to neighbor
.....
Please Input the code of command to be excute(0-17): 12
input 12 , Select send-community option .
```

To configure the community attribute for route, perform the following tasks:

| Step | Command                                  | Purpose                        |
|------|------------------------------------------|--------------------------------|
| 1.   | route-map map-name sequence-number {deny | Configure route map.           |
| 2.   | permit}                                  | Configure setting rules.       |
| 3.   | set community community-value            | Enter the router configuration |
| 4.   | router bgp autonomous-system             | mode.                          |

|                                         |                      |
|-----------------------------------------|----------------------|
| neighbor {ip-address   peer-group-name} | Apply route mapping. |
| route-map access-list-name {in   out }  |                      |

**Step1 :**

In the global directory input route-map Command,prompt is as below:

```
(00)WORD          Name of route-map
Please Input the code of command to be excute(0-0): 0
input 0 ,Select WORD option ,prompt is as below:
Please input a string:
input string , then prompt is as below:
(00)<1-65535>      Route-map sequence number
(01)deny          Route-map denies operations
(02)permit        Route-map permits operations
(03)<cr>
Please Input the code of command to be excute(0-3): 0
input 0 , specify sequence-number value , prompt is as below:
(00)deny          Route-map denies operations
(01)permit        Route-map permits operations
(02)<cr>
Please Input the code of command to be excute(0-2):
Select parameter .
```

**Step2 :**

In the prompt Select 13 option , prompt is as below:

```
(00)aggregator    BGP aggregator attribute
(01)as-path       BGP as-path attribute
(02)atomic-aggregate BGP atomic aggregate attribute
(03)community     BGP community attribute
.....
Please Input the code of command to be excute(0-13): 3
input 3 ,Select community option , prompt is as below:
(00)aa:nn         Community number in aa:nn format
(01)<1-4294967295> Community number
(02)local-AS      Not send outside local AS (Well known community)
(03)no-advertise  Not send to any peer (Well known community)
(04)no-export     Not send outside AS/confederation (Well known community)
Please Input the code of command to be excute(0-4): 1
input 1 , then prompt is as below:
Please input a digital number:Please input a string:
确定 community-value value , prompt is as below:
(00)aa:nn         Community number in aa:nn format
(01)<1-4294967295> Community number
(02)local-AS      Not send outside local AS (Well known community)
(03)no-advertise  Not send to any peer (Well known community)
(04)no-export     Not send outside AS/confederation (Well known community)
(05)<cr>
Please Input the code of command to be excute(0-5): 5
input 5 , confirm it.
```

**Step3 :**

In the prompt Select 12 option , prompt is as below:

```
(00)beigrp        Enable BEIGRP (compatible with eigrp)
```

```
(01)bgp          Enable Border Gateway Protocol (BGP)
(02)ospf         Enable Open Shortest Path First (OSPF)
(03)rip          Enable Routing Information Protocol(RIP)
Please Input the code of command to be excute(0-3): 1
input 1 ,Select bgp option ,prompt is as below:
(00)<1-65535>    Local anonymous system number
Please Input the code of command to be excute(0-0): 0
Select 0 ,prompt is as below:
Please input a digital number:Please input a string:
input autonomous-system value .
```

Step4 :

In the prompt Select 12 option , prompt is as below:

```
(00)A.B.C.D      IP address of neighbor
Please Input the code of command to be excute(0-0): 0
input 0 ,Select A.B.C.D option , then prompt :
Please input a IP Address:
input IP ,prompt is as below:
(00)default-originate    Permit announcement of default route to neighbor
.....
(09)route-map            Apply route map to the neighbor
.....
Please Input the code of command to be excute(0-17): 9
input 9 ,Select route-map option ,prompt is as below:
(00)WORD              Name of route-map
Please Input the code of command to be excute(0-0): 0
input 0 ,Select WORD option ,prompt is as below:
Please input a string:
input string , then prompt is as below:
(00)in                Map incoming routes
(01)out               Map outgoing routes
Please Input the code of command to be excute(0-1):
Select parameter .
```

Perform the following tasks for filter the route information base on community attribute:

| Step | Command                                                                                                                               | Purpose                              |
|------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 1.   | <code>ip community-list <i>community-list-name</i> {permit   deny} <i>communtiy-expression</i></code>                                 | Define community list.               |
| 2.   | <code>route-map <i>map-name</i> <i>sequence-number</i> {deny   permit}</code>                                                         | Configure route mapping.             |
| 3.   | <code>match community-<i>list-name</i></code>                                                                                         | Configure match rules.               |
| 4.   | <code>router bgp <i>autonomous-system</i></code>                                                                                      | Enter the router configuration mode. |
| 5.   | <code>neighbor {<i>ip-address</i>   <i>peer-group-name</i>}</code><br><code>route-map <i>config-route-map-name</i> {in   out }</code> | Apply route mapping.                 |

Step1 :

In global configure directory input **ip**Command , prompt is as below:

```
(00)access-list    Named access-list
(01)as-path       BGP as-path access list definition
(02)community-list    Community attribute list definition
```

.....

Please Input the code of command to be excute(0-20): **2**

input 2 , Select community-list option , prompt is as below:

(00)WORD                    Name of community-list

Please Input the code of command to be excute(0-20): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:

input string , then prompt is as below:

(00)deny Community list for denies

(01)permit Community list for permits

Please Input the code of command to be excute(0-20):

Select parameter item , and confirm the *communtiy-expression* value .

Step2 :

input **route-map** Command,prompt is as below:

(00)WORD                    Name of route-map

Please Input the code of command to be excute(0-0): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:

input string , then prompt is as below:

(00)<1-65535>                Route-map sequence number

(01)deny                      Route-map denies operations

(02)permit                    Route-map permits operations

(03)<cr>

Please Input the code of command to be excute(0-3): **0**

input 0 , *sequence-number* value , prompt is as below:

(00)deny                      Route-map denies operations

(01)permit                    Route-map permits operations

(02)<cr>

Please Input the code of command to be excute(0-2):

Select parameter .

Step3 :

In the prompt Select 8 option , prompt is as below:

(00)as-path                    Match as-path list

(01)community                Match community list

(02)ip                         Match ip attribute

.....

Please Input the code of command to be excute(0-5): **1**

input 1 , Select community option , prompt is as below:

(00)WORD                    Name of community list

Please Input the code of command to be excute(0-0): **0**

input 0 , Select WORD option , prompt is as below:

Please input a string:

input *community-list-name*string

Step4 :

In the prompt Select 12 option , prompt is as below:

(00)beigrp                    Enable BEIGRP (compatible with eigrp)

(01)bgp                        Enable Border Gateway Protocol (BGP)

(02)ospf                        Enable Open Shortest Path First (OSPF)

(03)rip                         Enable Routing Information Protocol(RIP)

Please Input the code of command to be excute(0-3): **1**  
 input 1 , Select bgp option , prompt is as below:  
 (00)<1-65535> Local anonymous system number  
 Please Input the code of command to be excute(0-0): **0**  
 Select 0 , prompt is as below:  
 Please input a digital number:Please input a string:  
 input *autonomous-system* value .

Step5 :

In the prompt Select 12 option , prompt is as below:

(00)A.B.C.D IP address of neighbor  
 Please Input the code of command to be excute(0-0): **0**  
 input 0 , Select A.B.C.D option , then prompt 为 :  
 Please input a IP Address:  
 input IP , prompt is as below:  
 (00)default-originate Permit announcement of default route to neighbor  
 .....  
 (09)route-map Apply route map to the neighbor  
 .....

Please Input the code of command to be excute(0-17): **9**  
 input 9 , Select route-map option , prompt is as below:  
 (00)WORD Name of route-map  
 Please Input the code of command to be excute(0-0): **0**  
 input 0 , Select WORD option , prompt is as below:  
 Please input a string:  
 input string , then prompt is as below:  
 (00)in Map incoming routes  
 (01)out Map outgoing routes  
 Please Input the code of command to be excute(0-1):  
 Select parameter .

See the “[BGP Community Attribute Route Mapping Example](#)” section for examples of BGP community attribute.

**Configure Autonomous System Confederation**

One way to reduce the IBGP mesh is to divide an autonomous system into multiple sub-autonomous systems and group them into a single confederation. To the outside world, the confederation looks like a single autonomous system. Each sub-autonomous system is fully meshed within itself, and has a few connections to other sub-autonomous systems in the same confederation. Even though the peers in different autonomous systems have EBGP sessions, they exchange routing information as if they were IBGP peers. Specifically, the next-hop, MED, and local preference information is preserved.

To configure a BGP autonomous system confederation, you must specify a confederation identifier. A confederation identifier is a number of autonomous system. To the outside world, the group of autonomous systems will look like a single autonomous system with the confederation identifier as the autonomous system number.

To configure an autonomous system confederation identifier, use the following BGP configuration command in router configuration mode:

| Command                                                   | Purpose                                                  |
|-----------------------------------------------------------|----------------------------------------------------------|
| bgp confederation0 identifier<br><i>autonomous-system</i> | Configure an autonomous system confederation identifier. |

In the prompt Select 1 option , prompt is as below:  
 (00)always-compare-med Always compare MED  
 .....

(04)confederation AS confederation

.....

Please Input the code of command to be excute(0-8): **4**

input 4 , Select confederation option , prompt is as below:

(00)identifier AS number of AS confederation

(01)peers AS confederation members

Please Input the code of command to be excute(0-1): **0**

input 0 , Select identifier option , prompt is as below:

(00)<1-65535> AS number

Please Input the code of command to be excute(0-0): **0**

Select 0 , then prompt is as below:

Please input a digital number:Please input a string:

input *autonomous-system* value

To specify the autonomous system number that belong to an autonomous system confederation, use the following BGP configuration command:

| Command                                                                                    | Purpose                                                                           |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <pre>bgp confederation peers <i>autonomous-system</i> [<i>autonomous-system ...</i>]</pre> | Specify the autonomous system that belongs to an automomous system confederation. |

In the prompt Select 1 option , prompt is as below:

(00)always-compare-med Always compare MED

.....

(04)confederation AS confederation

.....

Please Input the code of command to be excute(0-8): **4**

input 4 , Select confederation option , prompt is as below:

(00)identifier AS number of AS confederation

(01)peers AS confederation members

Please Input the code of command to be excute(0-1): **1**

input 0 , Select peers option , prompt is as below:

(00)<1-65535> AS number

Please Input the code of command to be excute(0-0): **0**

Select 0 , then prompt is as below:

Please input a digital number:Please input a string:

input *autonomous-system* value

See the “[BGP Autonomous System Confederation Example](#)” for examples of autonomous system confederation.

### Configure a Route Reflector

Instead of configuring a autonomous system confederation, another way to reduce the IBGP mesh is to configure a route reflector.

The internal peers of the route reflector are divided into two groups: client peers and all the other routers in the autonomous system (nonclient peers). A route reflector reflects routes between these two groups. The route reflector and its client peers form a cluster. The nonclient peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with IBGP speakers outside their cluster.

When the route reflector receives an advertised route, it takes the following actions:

1. A route from an external BGP speaker is advertised to all clients and nonclient peers.
2. A route from a nonclient peer is advertised to all clients.

3. A route from a client is advertised to all clients and nonclient peers. Hence, the clients need not be fully meshed. To configure a route reflector and its clients, perform the following task in router configuration mode:

| Command                                                      | Purpose                                                                                     |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>neighbor <i>ip-address</i><br/>route-reflector-client</b> | Configure the local router as a BGP route reflector and the specified neighbor as a client. |

In the prompt Select 12 option , prompt is as below:

```
(00)A.B.C.D          IP address of neighbor
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option , then prompt :
Please input a IP Address:
input IP , prompt is as below:
(00)default-originate      Permit announcement of default route to neighbor
.....
(10)route-reflector-client  Configure the neighbor as route reflector client
.....
Please Input the code of command to be excute(0-17): 10
input 10 , Select route-reflector-client option .
```

An autonomous system can have multiple route reflectors. A route reflector treats other route reflectors just like other IBGP speakers.

Usually a cluster of clients will have a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. To increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. All the route reflectors serving a cluster should be fully meshed and all of them should have identical sets of client and nonclient peers.

If the cluster has more than one route reflector, configure the cluster ID by performing the following task in router configuration mode:

| Command                                 | Purpose               |
|-----------------------------------------|-----------------------|
| <b>bgp cluster-id <i>cluster-id</i></b> | Configure cluster ID. |

In the prompt Select 1 option , prompt is as below:

```
(00)always-compare-med      Always compare MED
.....
(03)cluster-id             Route reflector cluster identifier
.....
Please Input the code of command to be excute(0-8): 3
input 3 , Select cluster-id option , prompt is as below:
(00)A.B.C.D              IP address
(01)<1-4294967295>       ID number
Please Input the code of command to be excute(0-1):
Select parameter , cluster-id value .
```

See the “[BGP route reflector configuration example](#)“ for an example of route reflector configuration.

### Disable Peer

Use the following BPG configuration command to disable BGP neighbor:

| Command                                                               | Purpose               |
|-----------------------------------------------------------------------|-----------------------|
| <b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>} shutdown</b> | Disable BGP neighbor. |

In the prompt Select 12 option , prompt is as below:

(00)A.B.C.D IP address of neighbor  
 Please Input the code of command to be excute(0-0): **0**  
 input 0 , Select A.B.C.D option , then prompt 为 :  
 Please input a IP Address:  
 input IP , prompt is as below:  
 (00)default-originate Permit announcement of default route to neighbor  
 .....  
 (13)shutdown Shutdown neighbor  
 .....  
 Please Input the code of command to be excute(0-17): **13**  
 input 13,Select shutdown option .

Use the following BPG configuration command to enable the the neighbor that former disabled:

| Command                                                        | Purpose              |
|----------------------------------------------------------------|----------------------|
| <b>neighbor (undo) {ip-address / peer-group-name} shutdown</b> | Enable BGP neighbor. |

In the prompt Select 12 option , prompt is as below:

U(undo) D(default) Q(quit)  
 (00)A.B.C.D IP address of neighbor  
 Please Input the code of command to be excute(0-0): **d**  
 First input D or d , then prompt is as below:  
 (00)A.B.C.D IP address of neighbor  
 Please Input the code of command to be excute(0-0): **0**  
 input 0 , Select A.B.C.D option , then prompt 为 :  
 Please input a IP Address:  
 input IP , prompt is as below:  
 (00)default-originate Permit announcement of default route to neighbor  
 .....  
 (13)shutdown Shutdown neighbor  
 .....  
 Please Input the code of command to be excute(0-17): **13**  
 input 13,Select shutdown option .

### Configure Multi-Hop External Peer

By default, external peer group must be in network directly connected. Perform command below to configure multi-Hop external peer group:

| Command                                                          | Purpose                                                     |
|------------------------------------------------------------------|-------------------------------------------------------------|
| <b>neighbor {ip-address / peer-group-name} ebgp-multihop ttl</b> | Configure BGP neighbor to be multi-Hop external peer group. |

In the prompt Select 12 option , prompt is as below:

(00)A.B.C.D IP address of neighbor  
 Please Input the code of command to be excute(0-0): **0**  
 input 0 , Select A.B.C.D option , then prompt 为 :  
 Please input a IP Address:  
 input IP , prompt is as below:  
 (00)default-originate Permit announcement of default route to neighbor  
 .....  
 (03)ebgp-multihop Allow EBGp neighbor not directly connected  
 .....  
 Please Input the code of command to be excute(0-17): **3**  
 input 3,Select ebgp-multihop option , prompt is as below:

(00)<1-255> Maximum hop count  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , prompt is as below:  
 Please input a digital number:Please input a string:  
 input *ttl* value .

**Set Administrative Distance**

Administrative distance is a measure of the preference of different routing protocols. BGP uses three different administrative distances: external, internal, and local. Routes learned through external BGP are given the external distance, routes learned with internal BGP are given the internal distance, and routes that are part of this autonomous system are given the local distance. To assign a BGP administrative distance, perform the following task in router configuration mode:

| Command                                                                                 | Purpose                               |
|-----------------------------------------------------------------------------------------|---------------------------------------|
| <b>distance bgp</b> <i>external-distance</i><br><i>internal-distance local-distance</i> | Assign a BGP administrative distance. |

In the prompt Select 5 option , prompt is as below:

(00)<1-255> Administrative distance of routes  
 (01)bgp Distance of BGP routes  
 Please Input the code of command to be excute(0-1): 1  
 input 1 , Select bgp option , prompt is as below:  
 (00)<1-255> Distance for routes external to the AS  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , prompt is as below:  
 Please input a digital number:Please input a string:  
 input *external-distance* value , prompt is as below:  
 (00)<1-255> Distance for routes internal to the AS  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , prompt is as below:  
 Please input a digital number:Please input a string:  
 input *internal-distance* value , prompt is as below:  
 (00)<1-255> Distance for local routes  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , prompt is as below:  
 Please input a digital number:Please input a string:  
 input *local-distance* value .

Changing the administrative distance of BGP routes is considered dangerous and generally is not recommended. The external distance should be lower than any other dynamic routing protocol, and the internal and local distances should be higher than any other dynamic routing protocol.

**Adjust BGP Timers**

To adjust BGP timer **keepalive** and **holdtime** of a specified neighbor, perform the following task in router configuration mode:

| Command                                                                                                              | Purpose                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>config-neighbor</b> [ <i>ip-address / peer</i><br><i>group-name</i> ] <b>set-timers</b> <i>keepalive holdtime</i> | Adjust BGP timer <b>keepalive</b> and <b>holdtime</b> of a specified peer unit or group. (Count in second) |

In the prompt Select 12 option , prompt is as below:

(00)A.B.C.D IP address of neighbor  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select A.B.C.D option , then prompt 为 :

Please input a IP Address:

input IP , prompt is as below:

(00)default-originate Permit announcement of default route to neighbor

.....

(15)timers Configure BGP timers

.....

Please Input the code of command to be excute(0-17): **15**

input 15,Select timers option , prompt is as below:

(00)<0-65535> Keepalive interval

Please Input the code of command to be excute(0-0): **0**

input 0 , prompt is as below:

Please input a digital number:Please input a string:

input *keepalive* value , prompt is as below:

(00)<0-65535> Holdtime

Please Input the code of command to be excute(0-0): **0**

input 0 , prompt is as below:

Please input a digital number:Please input a string:

input holdt ime value

Use **neighbor (default) timers** command to revert BGP timer of a neighbor or peer group to be default value.

### Base Path Select ion on MEDs from Other Autonomous Systems

The MED is one of the parameters that is considered when select ing the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

By default, during the best-path select ion process, MED comparison is done only among paths from the same autonomous system. You can allow comparison of MEDs among paths regardless of the autonomous system from which the paths are received.

To do so, perform the following BGP configuration command:

| Command                       | Purpose                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------|
| <b>bgp always-compare-med</b> | Allow the comparison of MEDs for paths from neighbors in different autonomous systems. |

In the prompt Select 1 option , prompt is as below:

(00)always-compare-med Always compare MED

.....

(03)cluster-id Route reflector cluster identifier

.....

Please Input the code of command to be excute(0-8): **0**

input 0 , Select always-compare-med option

### 5.10.12 Monitor and Maintain BGP

The administrator can display and delete the content in BGP routing table or other databases, and can also display the detailed statistic information.

#### Clear the BGP Routing Table and Databases

The following table lists the tasks concerned with clearing the cache, the table or the BGP databases. Use these commands in management mode:

| Command                    | Purpose                                              |
|----------------------------|------------------------------------------------------|
| <b>rm ip bgp *</b>         | Reset all BGP connection.                            |
| <b>rm ip bgp as-number</b> | Reset the BGP connection of the specified autonomous |

|                                          |                                                                   |
|------------------------------------------|-------------------------------------------------------------------|
| <b>rm ip bgp address</b>                 | system.                                                           |
| <b>rm ip bgp address soft { in out }</b> | Reset the BGP connection of the specified neighbor.               |
| <b>rm ip bgp aggregates</b>              | Clear the inbound or outbound database of the specified neighbor. |
| <b>rm ip bgp networks</b>                | Clear the route generated by the route summary.                   |
| <b>rm ip bgp config- redistribute</b>    | Clear the route generated by the network command.                 |
|                                          | Clear the route generated by the forwarding.                      |

Take the first command for an example. :

input **clear** Command , prompt is as below:

- (00)arp-cache                      Clear the entire ARP cache
- (01)dialer                          Clear dialer statistics
- (02)frame-relay-inarp            Clear inverse ARP entries from the map table
- (03)ip                                IP

.....

Please Input the code of command to be excute(0-11): **3**

input 3 , Select ip option , prompt is as below:

- (00)beigrp                      Clear BEIGRP
- (01)bgp                              BGP information
- (02)dhcpd                        DHCP Server information

.....

Please Input the code of command to be excute(0-5): **1**

input 1 , Select bgp option , then prompt is as below:

- (00)\*                                Clear all peers
- (01)<1-65535>                    Clear peers by specified AS number
- (02)A.B.C.D                        IP address of neighbor to clear

.....

Please Input the code of command to be excute(0-7): **0**

input 0 , Select all option , prompt is as below:

- (00)soft Soft reconfigure
- (01)<cr>

Please Input the code of command to be excute(0-1): **1**

input 1 and confirm it.

**Display the Routing Table Information and the System Statistic Information**

You can display the detailed statistic information such as BGP routing table, databases, etc. The information can be used to decide the resource usage and to resolve the network problems. You can also display the reachability information.

Use the following management commands to show various routing statistic information:

| Command                                                                                                                      | Purpose                                                                            |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>show ip bgp</b>                                                                                                           | Show the BGP routing table in system.                                              |
| <b>show ip bgp prefix</b>                                                                                                    | Display the routes matching the specified prefix list.                             |
| <b>show ip bgp community</b>                                                                                                 | Display the statistic information of the community attribute.                      |
| <b>show ip bgp regexp</b><br><i>regular-expression</i>                                                                       | Display the routes matching the specified regular expression.                      |
| <b>show ip bgp network</b>                                                                                                   | Display the specified BGP route.                                                   |
| <b>show ip bgp neighbors address</b><br>show ip bgp neighbors [address]<br>[received-routes   routes  <br>advertised-routes] | Display the detailed TCP and BGP connection information of the specified neighbor. |
| <b>show ip bgp paths</b>                                                                                                     | Display the routes got from the special BGP neighbor.                              |
|                                                                                                                              | Display all BGP routing information in the database.                               |

**show ip bgp summary**

Display the status of the all BG connections.

input show Command , prompt is as below:

(00)alias                    alias for command

.....

(18)ip                        IP information

.....

Please Input the code of command to be excute(0-45): 18

input 18 , Select ip option , prompt is as below:

(00)access-lists            List IP access lists

(01)as-path-list            Information of AS-Path list

(02)beigrp                  Show BEIGRP information

(03)bgp                      BGP information

.....

Please Input the code of command to be excute(0-20): 3

input 3 , Select bgp option , prompt is as below:

(00)community              All BGP community information

(01)dampened-paths         Display paths suppressed due to dampening

(02)filter-list             Display routes matching the aspath-list

.....

(10)<cr>

Please Input the code of command to be excute(0-10):

Select display information .

Trace the BGP information

With tracing the BGP information, you can observe the process of setting up the BGP connection and the process of receiving / transmitting the routes. Thereby you can locate the errors and resolve the problems.

Following is the trace commands:

| Command                       | Purpose                           |
|-------------------------------|-----------------------------------|
| <b>debug ip bgp *</b>         | Trace the common BGP information. |
| <b>debug ip bgp all</b>       | Trace all BGP information.        |
| <b>debug ip bgp fsm</b>       | Trace the BGP state machine.      |
| <b>debug ip bgp keepalive</b> | Trace the BGP Keepalive messages. |
| <b>debug ip bgp open</b>      | Trace the BGP Open messages.      |
| <b>debug ip bgp update</b>    | Trace the BGP Update messages.    |

input **debug** Command , prompt is as below:

(00)aaa                      Debug AAA process information

.....

(12)ip                        IP information

.....

Please Input the code of command to be excute(0-27): **12**

input 12 , Select ip option , prompt is as below:

(00)all                      All BGP information

(01)dampening              BGP route dampening

(02)event                    BGP events

.....

Please Input the code of command to be excute(0-8):

Select 调试 option .

### 5.10.13 BGP Configuration Example

Sections below supply examples of BGP configuration:

#### Examples of BGP Route Map

The following example shows how you can use route maps to modify incoming data from a neighbor. Any route received from 140.222.1.1 that matches the filter parameters set in autonomous system access list 200 will have its weight set to 200 and its local preference set to 250, and it will be accepted.

```
router bgp 100
!
 neighbor 140.222.1.1 route-map fix-weight in
 neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight permit 10
 match as-path aaa
 set local-preference 250
 set weight 200
!
ip aspath-list aaa permit ^690$
ip aspath-list aaa permit ^1800
```

In the following example, route map freddy marks all paths originating from autonomous system 690 with a Multi Exit Discriminator (MED) metric attribute of 127. The second permit clause is required so that routes not matching autonomous system path list 1 will still be sent to neighbor 1.1.1.1.

```
router bgp 100
 neighbor 1.1.1.1 route-map freddy out
!
ip aspath-list abc permit ^690_
ip aspath-list xyz permit .*
!
route-map freddy permit 10
 match as-path abc
 set metric 127
!
route-map freddy permit 20
 match as-path xyz
```

The following example shows how you can use route maps to modify incoming data from the IP forwarding table:

```
router bgp 100
 redistribute rip route-map rip2bgp
!
route-map rip2bgp
 match ip address rip
 set local-preference 25
 set metric 127
 set weight 30000
 set next-hop 192.92.68.24
 set origin igp
!
ip access-list standard rip
```

```

permit 131.108.0.0 255.255.0.0
permit 160.89.0.0 255.255.0.0
permit 198.112.0.0 255.255.128.0

```

### BGP Neighbor Configuration Examples

In the following example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The first router listed is in a different autonomous system; the second neighbor command specifies an internal neighbor (with the same autonomous system number); and the third neighbor command specifies a neighbor on a different autonomous system.

```

router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99

```

### Examples of BGP Route Filtering by Neighbor

The following is an example of BGP path filtering by neighbor. The routes that pass **as-path** access list 1 will get weight 100. Only the routes that pass **as-path** access list 2 will be sent to 193.1.12.10. Similarly, only routes passing access list 3 will be accepted from 193.1.12.10.:

```

router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list test1 weight 100
neighbor 193.1.12.10 filter-list test2 out
neighbor 193.1.12.10 filter-list test3 in
ip aspath-list test1 permit _109_
ip aspath-list test2 permit _200$
ip aspath-list test2 permit ^100$
ip aspath-list test3 deny _690$
ip aspath-list test3 permit .*

```

### BGP Route Filtering base on Port Example

The following is an example of BGP path filtering by neighbor. The routes from port e1/O will be filtered by access list ac1.

```

router bgp 122
filter e1/0 in access-list ac1

```

Following example filters routes from port s1/O through using access list filter-network to filter network number as well as using access list filter-gateway to filter gateway address:

```

router bgp 100
filter s1/0 in access-list filter-network gateway filter-gateway

```

Following example filters routes from all ports through using prefix list filter-prefix to filter network number as well as using access list filter-gateway to filter gateway address:

```

router bgp 100
filter * in prefix-list filter-prefix gateway filter-gateway

```

### Examples of Route Filtering through Prefix List

Following example denies default route 0.0.0.0/0:

```
ip prefix-list abc deny 0.0.0.0/0
```

Following example allows routes matching prefix 35.0.0.0/8

```
ip prefix-list abc permit 35.0.0.0/8
```

In following example BGP process will only accept prefix length from /8 to /24:

```
router bgp
network 101.20.20.0
filter * in prefix max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

In following configuration, router will filter routes from all ports except of route whose prefix is in the range of 8-24:

```
router bgp 12
filter * in prefix-list max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

The following are examples of other prefix list configurations.

Following example allows route whose prefix length not larger than 24 in net 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

Following example denies route whose prefix length larger than 25 in net 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

Following example allows route whose prefix length larger than 8 and less than 24 in the whole address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

Following example denies route whose prefix length larger than 25 in the whole address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

Following example denies all routes of net 10/8. If the mask of A-class net 10.0.0.0/8 is less than or equal to 32 bits, it will deny all routes:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

Following example denies route whose mask length larger than 25 in net 204.70.1/24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

Following example allows all routes:

```
ip prefix-list abc permit any
```

### BGP Aggregate Route Examples

The following examples show how you can use aggregate routes in BGP either by redistributing an aggregate route into BGP or by using the conditional aggregate routing feature.

In the following example, the **redistribute static** command is used to redistribute aggregate route 193.\*.\*.\*:

```
ip route 193.0.0.0 255.0.0.0 null 0
!
router bgp 100
redistribute static
```

The following configuration creates an aggregate entry in the BGP routing table when there is at least one specific route that falls into the specified range. The aggregate route will be advertised as coming from your autonomous system and has the **atomic** aggregate attribute set to show that information might be missing.

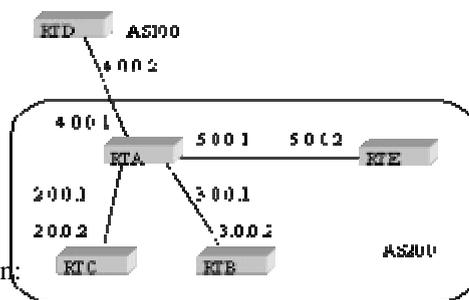
```
router bgp 100
aggregate 193.0.0.0/8
```

The following example not only creates the aggregate route for 193.\*.\*.\*, but will also suppress advertisements of more specific routes to all neighbors:

```
router bgp 100
aggregate 193.0.0.0/8 summary-only
```

### Examples of BGP Route Reflector Configuration

The following is an example of route reflector. RTA, RTB, RTC and RTE belong to the same Autonomous System AS200. RTA acts as route reflector. RTB and RTC are route reflector clients. RTE is a common IBGP neighbor. RTD belongs to AS100 and sets up a EBGP connection with RTA. Configuration is as following:



#### 1. RTA configuration:

```
interface s1/0
ip address 2.0.0.1 255.0.0.0
!
interface s1/1
ip address 3.0.0.1 255.0.0.0
!
interface s1/2
ip address 4.0.0.1 255.0.0.0
!
interface s1/3
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200 /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200 /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200 /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100 /*RTD EBGP*/
network 11.0.0.0/8
!
```

#### 2. RTB configuration:

```
interface s1/0
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
```

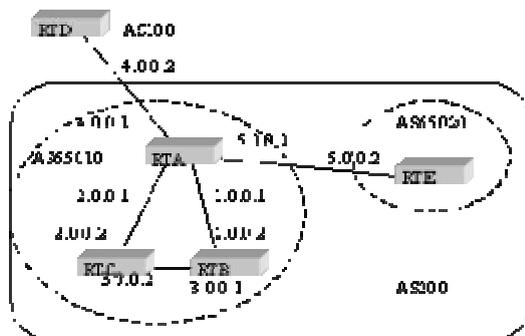
```

neighbor 3.0.0.1 remote-as 200 /*RTA IBGP*/
network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
3. RTC configuration:
interface s1/0
ip address 2.0.0.2 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200 /*RTA IBGP*/
network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12
4. RTD configuration:
interface s1/0
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200 /*RTA EBGP*/
network 14.0.0.0/8
!
ip route 14.0.0.0 255.0.0.0 4.0.0.12
5. RTE configuration:
interface s1/0
ip address 5.0.0.2 255.0.0.0
!
router bgp 200
neighbor 5.0.0.1 remote-as 200 /*RTA IBGP*/
network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12

```

**BGP AS Confederation Example**

The following is a configuration of Autonomous System Confederation. RTA, RTB and RTC are in IBGP connections and belong to private AS 65010. RTE belongs to private AS 65020. RTE builds interior EBGP connection with RTA in AS confederation. AS65010 and AS65020 buildup an AS confederation whose number is AS200. RTD belongs to Autonomous System AS100. RTD builds EBGP connection with AS200 through RTA.



```

1. RTA configuration:
interface s1/0
ip address 1.0.0.1 255.0.0.0

```

```
!  
interface s1/1  
ip address 2.0.0.1 255.0.0.0  
!  
interface s1/2  
ip address 4.0.0.1 255.0.0.0  
!  
interface s1/3  
ip address 5.0.0.1 255.0.0.0  
!  
router bgp 65010  
bgp confederation identifier 200  
bgp confederation peers 65020  
neighbor 1.0.0.2 remote-as 65010 /*RTB IBGP*/  
neighbor 2.0.0.2 remote-as 65010 /*RTC IBGP*/  
neighbor 5.0.0.2 remote-as 65020 /*RTE EBGP*/  
neighbor 4.0.0.2 remote-as 100 /*RTD EBGP*/  
2.RTB configuration:  
interface s1/0  
ip address 1.0.0.2 255.0.0.0  
!  
interface s1/1  
ip address 3.0.0.1 255.0.0.0  
!  
router bgp 65010  
bgp confederation identifier 200  
bgp confederation peers 65020  
neighbor 1.0.0.1 remote-as 65010 /*RTA IBGP*/  
neighbor 3.0.0.2 remote-as 65010 /*RTC IBGP*/  
3.RTC configuration:  
interface s1/0  
ip address 2.0.0.2 255.0.0.0  
!  
interface s1/1  
ip address 3.0.0.2 255.0.0.0  
!  
router bgp 65010  
bgp confederation identifier 200  
bgp confederation peers 65020  
neighbor 2.0.0.1 remote-as 65010 /*RTA IBGP*/  
neighbor 3.0.0.1 remote-as 65010 /*RTB IBGP*/  
4.RTD configuration:  
interface s1/0  
ip address 4.0.0.2 255.0.0.0  
!  
router bgp 100  
neighbor 4.0.0.1 remote-as 200 /*RTA EBGP*/  
5.RTE configuration:  
interface s1/0
```

```
ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
bgp confederation identifier 200
bgp confederation peers 65010
neighbor 5.0.0.1 remote-as 65010 /*RTA EBGP*/
```

### Examples of BGP Community Route Map

This section includes three examples of using route maps of BGP community.

In the first example, route map set-community is used for outbound updates getting to neighbor 171.69.232.50. Special community attribute “no-export” is set on routes passing access list aaa. Other routes will be advertised normally. This special community attribute will automatically forbid BGP session parts in AS200 to advertise this route to AS outside.

```
router bgp 100
neighbor 171.69.232.50 remote-as 200
neighbor 171.69.232.50 send-community
neighbor 171.69.232.50 route-map set-community out
!
route-map set-community 10 permit
match ip address aaa
set community no-export
!
route-map set-community 20 permit
```

In the second example, route map set-community is used for outbound updates getting to 171.69.232.90. All routing configurations generated by AS 70 will add the community attribute value 200 into current values. Other routes will be advertised normally.

```
route-map bgp 200
neighbor 171.69.232.90 remote-as 100
neighbor 171.69.232.90 send-community
neighbor 171.69.232.90 route-map set-community out
!
route-map set-community 10 permit
match as-path test1
set community-additive 200 200
!
route-map set-community 20 permit
match as-path test2
!
ip aspath-list test1 permit 70$
ip aspath-list test2 permit .*
```

In the third example, we will set MED of a route from neighbor 171.69.232.55 and set local priority according to community attribute value of this route. Those MEDs of routes matching community list com1 will be configured to be 8000. These routes maybe have other attributes.

The local priorities of routes transmitting community list com2 are configured to be 500.

The local priorities of other routes are configured to be 50. Therefore local priorities of the left routes of neighbor 171.69.232.55 are 50.

```
router bgp 200
neighbor 171.69.232.55 remote-as 100
neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
match community com1
set metric 8000
!
route-map filter-on-community 20 permit
match community com2
set local-preference 500
!
route-map filter-on-community 30 permit
set local-preference 50
!
ip community-list com1 permit 100 200 300
ip community-list com1 permit 900 901
!
ip community-list com2 permit 88
ip community-list com2 permit 90
!
```

## 5.11 Configure RSVP

This chapter describes how to configure Resource Reservation Protocol (RSVP), which is an IP service that allows end systems or hosts on either side of a router network to establish a reserved-bandwidth path between them to predetermine and ensure QoS for their data transmission.

For a complete description of the RSVP commands in this chapter, refer to the “RSVP Command” of IP Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

It is helpful for users to acquaint RSVP at first before configuring RSVP. RSVP allows end systems to request Quality of Service (QoS) guarantees for data flow of an application. RSVP also can be used by router to transfer QoS request and to create and maintain state for actual reservation. RSVP request will create reservation on every node of data passage.

RSVP request aims at half-duplex data flow, so RSVP will distinguish the data sender and the data receiver in logic in spite that sender and receiver are the same application. RSVP stands higher than IP in the whole protocol cluster. It doesn't transmit data, but it belongs to internet control protocol just like ICMP, IGMP or Routing Protocol. RSVP implementation functions on background as routing protocol or Management protocol.

RSVP per se is not routing protocol although it can meet current and future routing protocol. Routing protocol decides data packets how to forward and RSVP only cares QoS of those data packets forwarded according to route.

RSVP functions accordant with WFQ (Weighted Fair Queuing) or RED (Random Early Detection). This accordance is concerned with two primary concepts: using of RSVP point-to-point flow and using of session between WFQ routers.

### 5.11.1 How to Enable RSVP on Router

User should configure the interface on which RSVP will be enabled in command to enable RSVP on router. This can be implemented with commands of RSVP interface configuration. If user completes upper configurations on all interfaces

wanted RSVP, RSVP will function on these interfaces.

To enable RSVP on an interface, perform the following task in global configuration mode:

| Command                                                                        | Purpose                              |
|--------------------------------------------------------------------------------|--------------------------------------|
| <b>ip rsvp bandwidth</b> [ <i>interface-kbps</i> ] [ <i>single-flow-kbps</i> ] | Configure RSVP on network interface. |

In the prompt Select ip option , then prompt is as below:

```
(00)access-group          Specify access control for packets
.....
(14)rsvp                  RSVP interface command
.....
```

Please Input the code of command to be excute(0-18): 14

input 14 , Select rsvp option , prompt is as below:

```
(00)bandwidth            RSVP interface bandwidth setting
(01)tos                  RSVP TOS setting
(02)precedence           RSVP precedence setting
(03)neighbor             RSVP neighbor setting
```

Please Input the code of command to be excute(0-3): 0

input 0 , Select bandwidth option , prompt is as below:

```
(00)<1-1000000>          Amount of bandwidth (in kbps) on interface to be reserved
```

Please Input the code of command to be excute(0-0): 0

input 0 , and confirm it *interface-kbps* value , prompt is as below:

```
(00)<1-1000000>          Amount of bandwidth (in kbps) allocated to a single flow
```

Please Input the code of command to be excute(0-0): 0

input 0 , and confirm it *single-flow-kbps* value .

Note: When using ip rsvp bandwidth command, if interface-kbps and single-flow-kbp are omitted, the whole port can apply for upper limit of reservation resource, and single data flow can apply for an upper limit of reservation resource which is 75% of port resource by default.

### 5.11.2 How to Enable RSVP in IP Phone Module

Before configuring D-LINK IP Phone and D-LINK IP Phone module as well as use Voice over IP, user must enable RSVP in command to configure resource reservation for voice flow with RSVP:

Do configure RSVP commands on the port needing RSVP configuration because RSVP is disabled on port by default. (Refer to last section for usage.)

Because IP Phone disables QOS by default, user should enable QOS in dial-peer voip.

Use command below in dail-peer configuration state to enable RSVP on port f0/0:

| Command                                                      | Purpose                                      |
|--------------------------------------------------------------|----------------------------------------------|
| <b>req - qos { guarantee   load }</b> [ <i>flow - kbps</i> ] | Configure bandwidth for IP Phone voice flow. |

Note: In the default of guarantee | load, resource reservation form is guarantee. In the default of flow-kbps, reservation bandwidth is 24kbps.

### 5.11.3 Use RSVP Assistant Configuration Commands

On RSVP module implementation of current edition, user can process RSVP debug with assistant configuration commands, including setting up of RSVP session and transmitting information of RSVP path, path tear, resv, resv tear, offered by the module. This will affect very much on RSVP debug.

Use commands below in global configuration directory:

| Command                                                                                                                                                         | Purpose                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>ip rsvp local session</b> <i>session-ip-address session-dport</i> { <i>tcp</i>   <i>udp</i> }                                                                | With this command user can configure a new RSVP session which can be used by other commands.                       |
| <b>ip rsvp local sender</b> <i>session-id sender-ip-address sender-sport</i> [ <i>config-bw</i> ] [ <i>burst-size</i> ]                                         | This command makes user be able to send out path message. Form no of this command will send out path tear message. |
| <b>ip rsvp local reservation</b> <i>session-id sender-ip-address sender-sport</i> [ <b>guarantee</b>   <b>load</b> ] [ <i>config-bw</i> ] [ <i>burst-size</i> ] | This command makes user send out resv message. Form no of this command will send out resv tear message.            |

Take the first command for an example. :

```
input ip Command , prompt is as below:
(00)access-list          Named access-list
.....
(17)rsvp                  Configure RSVP information
.....
Please Input the code of command to be excute(0-20): 17
input 17 , Select rsvp option , prompt is as below:
(00)local                RSVP local configuartion
Please Input the code of command to be excute(0-0): 0
input 0 , Select local option , prompt is as below:
(00)session              RSVP Session configuartion
(01)sender                RSVP Sender configuartion
(02)reservation          RSVP Reservation configuartion
Please Input the code of command to be excute(0-2): 0
input 0 , Select session option , prompt is as below:
(00)A.B.C.D              Destination address
Please Input the code of command to be excute(0-0): 0
input 0 , Select A.B.C.D option , prompt is as below:
Please input a IP Address:
input IP , prompt is as below:
(00)<0-65535>            Destination port
Please Input the code of command to be excute(0-0): 0
input 0 , prompt is as below:
Please input a digital number:Please input a string:
input port value , prompt is as below:
(00)tcp                  TCP Transport
(01)udp                  UDP Transport
Please Input the code of command to be excute(0-0):
Select parameter .
```

#### 5.11.4 How to Configure TOS and Precedence for RSVP Flow

To get better implementation of reservation, user can use commands offered by RSVP module to set TOS and precedence of RSVP flow. This makes that a higher TOS is set when RSVP flow exceeds reservation and a lower TOS is set when flow is in a special range of reservation. Precedence is the same.

Use commands below in interface configuration state:

| Command                                                            | Purpose                                                               |
|--------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>ip rsvp tos</b> {conform exceed} <i>tos-value</i>               | This command can be used to configure TOS of reservation flow.        |
| <b>ip rsvp precedence</b> {conform exceed} <i>precedence-value</i> | This command can be used to configure Precedence of reservation flow. |

Take the first command for an example. :

In the prompt Select ip option , then prompt is as below:

```
(00)access-group          Specify access control for packets
.....
(14)rsvp                  RSVP interface command
.....
```

Please Input the code of command to be excute(0-18): 14

input 14 ,Select rsvp option ,prompt is as below:

```
(00)bandwidth            RSVP interface bandwidth setting
(01)tos                  RSVP TOS setting
(02)precedence           RSVP precedence setting
(03)neighbor             RSVP neighbor setting
```

Please Input the code of command to be excute(0-3): 1

input 1 ,Select tos option ,prompt is as below:

```
(00)conform              TOS conform setting
(01)exceed               TOS exceed setting
```

Please Input the code of command to be excute(0-1):

Select conform 与 exceedparameter ,then prompt is as below:

```
(00)<0-15>                TOS value setting
```

Please Input the code of command to be excute(0-0): 0

input 0 ,prompt is as below:

Please input a digital number:Please input a string:

input *tos-value* value.

### 5.11.5 How to Use access-list in RSVP module

When user configures RSVP on router, he is entitled to use access-list to allow or deny some hosts or routers to communicate with local router.

Use command below in interface configuration state to complete this function:

| Command                                         | Purpose                                                                                                                               |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip rsvp neighbor</b> <i>access-list-name</i> | If this command is configured, only the RSVP request of host conforming to access list will be accepted. Otherwise it will be denied. |

In the prompt Select ip option , then prompt is as below:

```
(00)access-group          Specify access control for packets
.....
(14)rsvp                  RSVP interface command
.....
```

Please Input the code of command to be excute(0-18): 14

input 14 ,Select rsvp option ,prompt is as below:

```
(00)bandwidth            RSVP interface bandwidth setting
```

```

(01)tos                RSVP TOS setting
(02)precedence        RSVP precedence setting
(03)neighbor          RSVP neighbor setting
Please Input the code of command to be excute(0-3): 3
input 1 ,Select neighbor option ,prompt is as below:
(00)WORD              Access-list name
Please Input the code of command to be excute(0-0): 0
input 0 ,Select WORD option ,prompt is as below:
Please input a string:
input access-list-namestring .

```

### Configure multicast-group route

multicast-group route overview

#### the implement of D-Link's multicast-group route

IGMP

OLNK

PIM-DM

Basic multicast-group route configuration task list

Advance multicast-group route configuration task list

Start multicast-group route

Start multicast-group route on the port

Start OLNK

Start PIM-DM

IGMP configuration task list

Configure TTL threshold

Cancel multicast-group fast transmit

Configure PIM-DM task list

Configure multicast-group static route

Control transmit speed to IGMP group

Configure IP multicast-group boundary

Configure IP multicast-group flow control

Configure IP multicast-group Helper

Configure stub multicast-group route

Watch and maintenance multicast-group route

Remove multicast-group buffer,route table

Display multicast-group route table and system statistic information

Example of multicast-group route configuration

Example of PIM-DM configuration

Example of PIM-DM state fresh configuration

Example of management boundary configuration

Example of multicast-group Helper configuration

Example of stub multicast-group

#### multicast-group route overview

This chapter introduce how to configure multicast-group route protocol.If you want to know the complete description of multicast-group route command of this chapter,please reference other chapter about “multicast-group route command”. Traditional IP transmission allow one host to other one(unicast communication) or all(broadcast communication), multicast-group technology provides the third choose,it allow a host send message to some hosts.These hosts are called group member.

The destination address of message send to group member is D class address (224.0.0.0—239.255.255.255).

Transmission of multicast-group message is similar to UDP. It is a best-effort service, and doesn't provide reliable transmission and error control which is provided by TCP.

The application which constitutes multicast-group needs sender and receiver. The sender need not join a group to send a multicast-group message, and that the receiver must join a group before it receives the message of this group.

The relation of the group member is dynamic, hosts could join and leave the group at any moment, also, the position and number of group member are not limited. If you need, a host can be a member of some groups at a time. So, the state of group and number of group member change as time goes by.

Routers execute multicast-group route protocol (e.g. PIM-DM, PIM-SM) in order to maintain the route table which is used to transmit multicast-group message, and use IGMP protocol to learn the states of the group member which connect to the same network. Hosts send IGMP report message in order to join in the specified IGMP group.

IP multicast-group technology is fit to "one to many" multimedia implement.

### The implement of D-Link's multicast-group

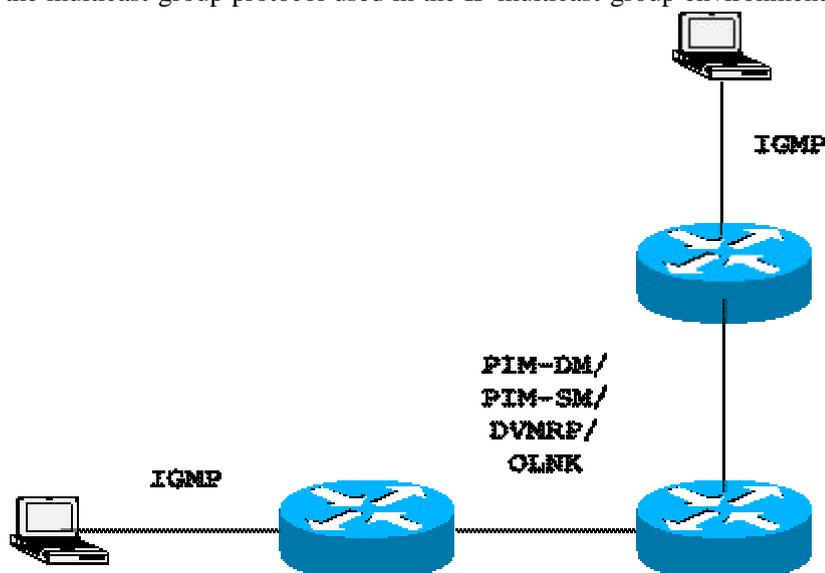
In the router software of D-Link, multicast-group route contain protocols as follow:

.IGMP run between router and host in the LAN, trace the relation of group member.

.OLNK is a static multicast-group technology used in simple topology structure, it not only implement multicast-group transmit, but also reduce the waste of CPU and bandwidth of multicast-group route protocol.

.PIM-DM/PIM-SM/DVMRP are dynamic multicast-group route protocol, run over the routers, they establish multicast-group route table in order to implement multicast-group transmission.

The following picture display the multicast-group protocol used in the IP multicast-group environment.



### IGMP

IGMP is a class protocol which aim at multicast group member management, IGMP is short for Internet Group Management Protocol. IGMP is an isomeric protocol, it consist host and router. The protocol of the host part regulate host how to report its own identity to the route and host how to respond to the Query message send by the router. The protocol of the router part regulate router which support IGMP how to obtain the host's group member identity in local network, and according to the report send by the host update group member's information which is saved by the router.

According to implement of IGMP router part protocol in our routers, it can provide the exist of present network multicast-group member to the multicast route protocol of the router. The protocol will determine whether to transmit multicast message. Generally speaking, in order to make our router support IP message multicast process, it need to implement multicast route protocol and IGMP router part protocol. Present, our router has implement IGMP router part protocol, which support the newest version—IGMP version 3.

In the actual implement, there is no sole start command which is aim at IGMP, IGMP router port function start from Multicast Routing Protocol.

### OLNK

Strictly speaking, OLNK (IGMP only-link) could not be called multicast-group route protocol, because it can't

provide interaction of protocol. But, run OLNK will obtain good effort under some specified situation and simple topology environment. It is similar to PIM-DM which couldn't provide interaction of protocol., and it can manage local IGMP group member's change, according to topology change adjust RPF interface, it will not only ensure the transmit of multi-cast , but also avoid the control message of multi-cast route protocol occupy the usage of bandwidth,

#### PIM-DM

PIM-DM(Protocol Independent Multicast Dense Mode) is a kind of multi-cast route protocol with compression mode, default considering, when multi-cast begin to send multi-cast data, network stations from the whole work place have to receive the data, so the PIM-DM will choose the diffuse-pruning to transmit the multi-cast data. When multi-cast source begin to transmit the data, the interface active by PIM along with router face to the RPF interface of the source will transmit the multi-cast data package. In this way, all network nodes of PIM-DM area will receive those multi-cast data package. In order to complete the multi-cast transmit, relative routers should create the multi-cast router item (s,g) for group G and its source S.(S,G) includes the source address , group address, entry address, exit address, timer and flags of multi-cast.

If there is no multi-cast member in some area in network, PIM-DM protocol will send pruning message, it will pruning at the transmit interface via the area and will build the pruning states which corresponding the overtime times. When the times overtime, the pruning states will return to transmit states again, and the multi-cast data will down along the branch again. Besides, pruning states includes multi-cast source and multi-cast group message. When the multi-cast group member happen in pruning area ,in order to reduce the response time ,protocol needn't wait for previous pruning states overtime, but send the engraft message to the previous actively to make the pruning states return to transmit states.

Once source S remain send message to group G, the first hop router will periodically send (S,G)states fresh information to next original broadcast tree to complete refurbish. The states fresh mechanism of PIM-DM could fresh lower states, so pruning of broadcast tree ramus will not overtime.

In the multiple access network, except refer to DR voting, PIM-DM bring in following mechanism: use assert mechanism to vote unique transmitter to prevent sending

#### **Basic multicast-group route configuration task list**

Basic multicast-group configuration include:

- . Start multicast-group route
- . Start multicast-group function on the port
- . Configure IGMP speciality (optional)
- . Configure TTL threshold (optional)
- . Cancel multicast-group fast transmit (optional)

#### **Advance multicast-group route configuration task list**

Advance multicast-group configuration include

- . Configure PIM-DM task list (optional)
- . Configure DVMRP task list (optional)
- . Configure multicast-group static route (optional)
- . Control the transmission speed of IGMP group (optional)
- . Configure multicast-group boundary (optional)
- . Configure multicast-group Helper (optional)
- . Configure Stub multicast-group route (optional)
- . Watch and maintenance multicast-group route (optional)

#### ◆ Start multicast-group route

Start multicast-group route in order to allow D-Link router software transmit multicast-group message. Under the global configuration catalog input the following command to start multicast-group message transmission:

| command | purpose |
|---------|---------|
|---------|---------|

|                                   |                             |
|-----------------------------------|-----------------------------|
| <code>ip multicast-routing</code> | Start multicast-group route |
|-----------------------------------|-----------------------------|

Input ip command,clew:

- (00) access-list            Named access-list
  - .....
  - (15) multicast-routing    Enable IP multicast forwarding
  - .....
- Please Input the code of command to be excute(0-25): **15**  
 Input 15 , select    multicast-routing option.

◆ Start multicast-group function on the port

Run multicast-group software on the port will activate IGMP operation. Multicast-group route protocol include OLNK,PIM-DM,PIM-SM, or DVMRP. On the same port ,it allow the only multicast-group protocol to run. Using D-Link router to connect some multicast-group domain, it can run different multicast-group protocol on the different port. Though D-Link router software could serve as multicast-group boundary router very well, if possible, please make sure that not run some multicast-group route protocol at the moment, because it will affect some other protocols. For example, when PIM-DM(only support (S,G) option) and BIDIR PIM-SM(only support (\*,G)option) running, it will lead to confusion.

Start OLNK

Running OLNK on the port in order to start multicast-group function. Under the port configuration input the following command:

| command              | purpose                     |
|----------------------|-----------------------------|
| <code>ip olnk</code> | Start multicast-group route |

In parameter clew choose the 17th option, clew:

- 00) access-group        Specify access control for packets
  - .....
  - (13) olnk                            start IGMP only-link on this interface
  - .....
- Please Input the code of command to be excute (0-22): **13**  
 input 11 , choose olnk option.

◆ Start PIM-DM

Running PIM-DM on the port in order to activate coarctation mode multicast-group function, process as the following steps:

| command                | purpose                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------|
| <code>ip pim-dm</code> | Come into the port need to run PIM-DM , activate PIM-DM multicast-group route process under the port configuration |

In parameter clew choose the 17th option, clew:

- (00) access-group        Specify access control for packets
- .....

(15) pim-dm PIM-DM interface commands

.....

Please Input the code of command to be excute(0-22): 15

Input 15 , choose pim-dm option.

### IGMP speciality configuration task list

The configuration commands of IGMP-Router port speciality mainly are adjust IGMP parameter command, following we will introduce the basic configuration command of IGMP-Router port. If you want to understand all the implement command of IGMP-Router port, please refer to the IGMP command explain document.

### Change IGMP version of present running

Since IGMP has been brought forward, there has been three official versions, corresponding to rfc1122, rfc2236, rfc3376. Thereinto, IGMP version 1 has just implemented the simplest multicast-group member record function; version 2 has implemented query function which aim at the specified multicast-group member and Leave message that IGMP host leave the specified multicast-group, reduce the delay of the group member change; version 3 has more implemented update and maintenance which corresponding to multicast-group member identity of the host source address, additional, version 3 IGMP Router has been fully compatible with the host port of version 1 and version 2,our router software system provides complete support for the IGMP Router port protocol of the three versions.

Since IGMP aims at configuration of router port, i.e. it could configure separately IGMP-Router port function (started by multicast-group route protocol which is configured on different port) on the different port, and could run different version IGMP on the different port.

Note: for the specified multicast-group router, on the different ports which connected to the same network, you could start the IGMP-Router function on one port.

If you want to change the IGMP-Router port protocol version, which is running on the port, and you can use the following command under the port configuration.

| step | command                        | purpose                                                     |
|------|--------------------------------|-------------------------------------------------------------|
| 1    | ip igmp version version_number | Change the version of IGMP which is running on current port |

Choose the 17th option in the parameter clew, notify

(00)access-group Specify access control for packets

.....

(06)igmp IGMP interface command

.....

Please Input the code of command to be excute(0-22): 6

input 6,choose igmp option, notify

.....

(07)static-group IGMP static multicast group

(08)version the IGMP version on the interface

Please Input the code of command to be execute (0-8): 8

input 8 , choose version option , notify :

(00)<1-3> the IGMP version number on the interface

Please Input the code of command to be execute (0-8):

Choose version.

### ◆ Example of change IGMP version

Because higher version IGMP-Router port protocol is compatible with the lower version IGMP host, so when lower version IGMP host exist in the network, it is not necessary to change the version of IGMP-Router port protocol which run

on the multicast-group router, but higher version IGMP-Router port protocol is not compatible with the lower version IGMP-Router port protocol, and suppose that there are routers which run lower version IGMP-Router port protocol in the network, it is necessary to change the IGMP-Router port protocol version on the correlation port of the router which run the higher version IGMP-Router port protocol, the principle of the change as follow: change all the different IGMP-Router port protocol version to the lowest IGMP-Router port protocol version.

If administrator knows that there are router which run IGMP-Router version 1 and router which run IGMP-Router version 2 in the network which connected to some port of the router, it is necessary to change the IGMP-Router protocol version on the corresponding port of the router which run the higher IGMP-Router version to 1. The following example demonstrate the process that administrator change the version which run on some port (the following example ethernet 0/0 port) to version 1.

```
interface ethernet 0/0
ip igmp version 1
```

**Configure IGMP query interval**

No matter what the version of the current IGMP-Router protocol, the multicast-group router will send IGMP General Query message every other time, the sending address is 224.0.0.1, the purpose is obtaining Report message which is responded by the IGMP host, and so could obtain the information about IGMP host in the network belong to which multicast-group. The interval time to send the General Query message is called IGMP Query Interval, if you set the time too long, and the router could not obtain the information about IGMP host in the network belong to which group quickly, if you set the time too short, it will increase the flow of IGMP message.

If you want to change IGMP Query Interval on some port, you can use the following command to change under the port configuration.

| step | command                     | purpose                                                        |
|------|-----------------------------|----------------------------------------------------------------|
| 1    | ip igmp query-interval time | change IGMP Query Interval on current port, the unit is second |

```
Choose the 17th option in the parameter clew, notify
(00) access-group      Specify access control for packets
.....
(06) igmp              IGMP interface command
.....
Please Input the code of command to be excute(0-22): 6
Input 6 , choose igmp option , notify :
(00)helper-address     relay igmp packet
.....
(05)query-interval     the interval between host query is sent
.....
Please Input the code of command to be excute(0-8): 5
Input 5 , choose query-interval option , input time.
```

**Example of configure IGMP Query Interval**

The following example demonstrate the process that the administrator change the IGMP Query Interval to 50 second on the specified port (Ethernet 0/0 port)

```
Interface ethernet 0/0]
ip igmp query-interval 50
```

**Configure IGMP Querier interval**

For the IGMP-Router port protocol version 2 and version 3, if exist routers, they run the same IGMP-Router port

protocol in the same network, it need to face the problem of querier select ion, the definit ion of querier is the router which could send the query message (in fact, the port on the router which start the IGMP-Router port protocol), under the normal running, there is only one querier in the same network, it means only one router could send IGMP Query message. For IGMP-Router port protocol version 1, there is no problem about querier select ion, because in IGMP-Router version 1, which router could send IGMP Query message is specified by multicast-group route protocol.

For the IGMP-Router port protocol version 2 and version 3, use the same querier select ion mechanism: the router which have the least ip address is the querier of the network. For the non-querier, it needs to save one clock which used to record the time querier existed, when the clock is overtime, non-querier change to querier, and then start sending IGMP Query message until the router receives the IGMP Query message which is sent by the router who have the less ip address, and the querier change to non-querier again.

For IGMP-Router port protocol version 2, other querier existance interval could be configured by the following command :

| step | command                      | Purpose                                                    |
|------|------------------------------|------------------------------------------------------------|
| 1    | ip igmp querier-timeout time | Configure other querier existence interval, unit is second |

Choose the 17th option in the parameter clew, notify

(00)access-group                   Specify access control for packets

.....

(06)igmp                            IGMP interface command

.....

Please Input the code of command to be excute(0-22): **6**

input 6 , choose igmp option , notify :

(00)helper-address                relay igmp packet

.....

(04)querier-timeout               other querier exist time

.....

Please Input the code of command to be excute(0-8): **4**

input 4 , choose querier-timeout option , then input time.

#### ◆ Example of configuring IGMP Querier Interval

The following example demonstrate the process that administrator change the IGMP Querier Interval on one port to 100s. interface ethernet 0/0

```
ip igmp querier-timeout 100
```

#### ◆ Configure IGMP max response time

For the IGMP-Router port protocol version 2 and version 3, when sending IGMP General Query message, there is special data domain which specify the max response time of IGMP host in the IGMP message, it means that IGMP host must send the response message for the General Query message in the max response time after it receive the IGMP General Query message. If the max response time is set too long, it will lead to the delay of the IGMP host multicast-group member identity change. If the max response time is set too short, it will lead to the large flow of IGMP message in the network.

**Note : IGMP max response time must less than the IGMP Query Interval, when using the configuration command, if max response time is more than the IGMP Query Interval, system will auto set the max response time to query-interval-1.**

For the IGMP-Router port protocol version 2 and version 3, set IGMP max response time could use the following command under the port configuration.

| step | command                              | purpose                                  |
|------|--------------------------------------|------------------------------------------|
| 1    | ip igmp query-max-response-time time | Configure IGMP max response time,/second |

Choose the 17th option in the parameter clew, notify

(00)access-group Specify access control for packets

.....

(06)igmp IGMP interface command

.....

Please Input the code of command to be excute(0-22): **6**

input 6 , choose igmp option , notify :

(00)helper-address relay igmp packet

.....

(06)query-max-response-time the max response time for group member to report

.....

Please Input the code of command to be execute (0-8): **6**

input 6 , choose query-max-response-time option , then input time .

For IGMP-Router port protocol version 1, the max response time is decided by the protocol, it can't be configured, so the front configuration command is not used in the IGMP-Router port protocol version 1.

◆ Example of configuring IGMP max response time

The following example demonstrate the process that administrator change the IGMP max response time on one port to 15s.

```
interface ethernet 0/0
ip igmp query-max-response-time 15
```

◆ Configure IGMP last member query interval

For the IGMP-Router port protocol version 2 and version 3, when send to someone specify Group Specific Query of multi-cast, it will take query interval of the last group member as the max response time of the master from IGMP Query message, that means the IGMP master must send the response message to Query message during the query interval of the last group member when receive the Group Specific Query. If the IGMP master check the state of itself, and fine that there is no need to response the Query message, then the response message will still not be sent after the interval, the multi-cast router will update the information about the members of multi-cast. If the interval is set too long, it will cause the delay that IGMP multi-cast members changes the status, while if the interval is too short, it will cause overflow of IGMP message.

For the IGMP-Router port protocol version 2 and version 3, set IGMP last group member query interval could use the following command under the port configuration:

| step | command                                 | Purpose                                              |
|------|-----------------------------------------|------------------------------------------------------|
| 1    | ip igmp last-member-query-interval time | configure IGMP last group member query interval (/s) |

Choose the 17th option in the parameter clew, notify

(00)access-group Specify access control for packets

.....

(06)igmp IGMP interface command

.....

Please Input the code of command to be execute (0-22): **6**

input 6 , choose igmp option , notify :

(00)helper-address relay igmp packet

.....

(03)last-member-query-interval the interval between host query is sent

.....

Please Input the code of command to be execute (0-8): **3**

input 3 , choose last-member-query-interval option , then input time.

For the IGMP-Router port protocol version 1, last group member query interval which is configured is not used, though, it could configure this command under the running IGMP version 1, but it does no effort.

### Example of Configuring IGMP last member query interval

The following example demonstrate the process that administrator change the IGMP last member query interval on one port to 2000ms.

```
interface ethernet 0/0
```

```
ip igmp last-member-query-interval 2000
```

### IGMP static configuration

In our implementation of IGMP\_Router end protocol, we also support static multicast group configuration on ports except those functions specified by the protocol. What is called “static” is to differentiate from “dynamic” information reported by IGMP host. As to an IGMP host, its multicast group membership may be variable. Given that it only belongs to multicast group group1 and wishes to receive multicast messages destined for multicast group group1. But after a while it might belong to multicast group group2 and wish to receive multicast messages destined for multicast group groups. And after a more while this IGMP host maybe belongs to none multicast group. So we said that the multicast group destining information reported by host is dynamic and variable.

Different from “Dynamic multicast group” described upward, if a certain port is statically configured to belong to a multicast group, then multicast group protocol will consider that this port will always need to receive those multicast messages destined for this multicast group unless you use command **no** to cancel this configuration. In addition, for the purpose of better consistency with IGMP\_Router protocol v3, static multicast group can specify receiving multicast messages from which source addresses, viz. increasing source-filter function of multicast message receiving.

You can use the following command in port configure to configure static multicast group on this port:

| Step | Command                                                                     | Purpose            |
|------|-----------------------------------------------------------------------------|--------------------|
| 1    | ip igmp static-group { *   group-address } {include source-address   <cr> } | 配置该 port 下的静态多播组属性 |

In the parameter prompt Select 17 option , prompt is as below:

(00)access-group Specify access control for packets

.....

(06)igmp IGMP interface command

.....

```

Please Input the code of command to be excute(0-22): 6
input 6 , Select igmp option , prompt is as below:
(00)helper-address          relay igmp packet
    .....
(07)static-group           IGMP static multicast group
    .....
Please Input the code of command to be excute(0-8): 7
input 7 , Select static-group option , prompt is as below:
(00)*                      Populated for all groups
(01)A.B.C.D                IP group address
Please Input the code of command to be excute(0-1):
Select attribute parameter .

```

#### Example of IGMP Static configuration

Static multicast-group configuration command could define different classes static multicast-group when it uses different parameters, the following example will introduce the results of using the different command parameters:

```

interface ethernet 0/0
ip igmp static -group *

```

the front configuration command configured static all the multicast-group on the ethernet 0/0 port, it means that the port belongs to all the multicast-group, multicast-group route protocol will send all the ip multicast message to this port.

```

interface ethernet 0/0
ip igmp static -group 224.1.1.7

```

the front configuration command configured static the multicast-group 224.1.1.7 on the ethernet 0/0 port, it means that the port belongs to the multicast-group 224.1.1.7, multicast-group route protocol will send all the ip multicast message to this port.

```

interface ethernet 0/0
ip igmp static -group 224.1.1.7 include 192.168.20.168

```

the front configuration command configured statically multicast-group 224.1.1.7 on the ethernet 0/0 port, and at the same time it defines the source-filter of the multicast-group is 192.168.20.168, it means that the port belongs to all the multicast-group, but it just only to accept the ip multicast message from 192.168.20.168, multicast-group route protocol will send ip multicast message which is from 192.168.20.168 to 224.1.1.7 to this port.

Aim at the front example, if you want to accept the ip multicast message which comes from 192.168.20.169 and send to 224.1.1.7, you could configure the following command under the port configuration.

```
ip igmp static -group 224.1.1.7 include 192.168.20.169
```

If you want to add source-filter information which aim at the multicast-group, you can execute the front command many times, define the different source-address.

**Note: when using the upper configuration command, you can not configure a multicast-group its multicast group information not only aims at a special source address, but also aims at all source addresses in the same multicast group at one time. Similarly, you can't configure a multicast group its group information not only aims at all source addresses, but also aims at a special source address in the same multicast group. If you do, the last command will be ignored. For an example, if you have configured command *ip igmp static-group 224.1.1.7*, and the next you configure command *ip igmp static-group 224.1.1.7 include 192.168.20.168*, then the last command will be ignored.**

#### Configure IGMP Immediate-leave list

If IGMP v2 has enabled on a port of your router, and only one IGMP host exists in the network this port connected with, then you can implement "Immediate Leave" of the IGMP host through configuring IGMP Immediate-leave list. As specified by IGMP v2, if a host wants to leave a special multicast group, this host will send Leave message to all multicast routers, and multicast routers will send out Group Specific message to acknowledge whether there has been no host needs to receive multicast messages destined for this multicast group. If you have configured "Immediate Leave", it will avoid

the message exchange between IGMP host and multicast routers, it can also avoid the delay of multicast group membership changing maintained by multicast routers.

**Note: This command can be configured either in global configuration or in port configuration, but in global configuration this command is prior than in port configuration. If you first configure this command in global configuration, then following configuring of this command in port configuration will be ignored. If you first configure this command in port configuration, then following configuring of this command in global configuration will cancel the command formerly configured in port configuration.**

As to IGMP-Router v2, you can use the following command to configure IGMP Immediate-leave list in port configuration:

| Step | Command                                      | Purpose                                                                                              |
|------|----------------------------------------------|------------------------------------------------------------------------------------------------------|
| 1    | ip igmp immediate-leave group-list list-name | Configure the access list for IGMP host which can implements "immediate leave from multicast group". |
| 2    | ip access-list standard list-name            | Create an IP standard access list whose name is list-name.                                           |
| 3    | permit source-address                        | Configure the IGMP hosts we wish to implement "immediate leave" in IP standard access list.          |

Step1 :

In the parameter prompt Select 17 option , prompt is as below:

```
(00)access-group          Specify access control for packets
```

```
.....
```

```
(06)igmp                  IGMP interface command
```

```
.....
```

Please Input the code of command to be excute(0-22): 6

input 6 , Select igmp option , prompt is as below:

```
(00)helper-address        relay igmp packet
```

```
(01)immediate-leave      leave groups immediately without sending query
```

```
.....
```

Please Input the code of command to be excute(0-8): 1

input 1 , Select immediate-leave option , prompt is as below:

```
(00)group-list           access list to specify groups
```

Please Input the code of command to be excute(0-0): 0

input 0 , Select group-list option , 在 input list-name .

Step2 :

In global configure directory input ipCommand , prompt is as below:

```
(00)access-list          Named access-list
```

```
(01)as-path              BGP as-path access list definition
```

```
.....
```

Please Input the code of command to be excute(0-22): 0

input 0 , Select access-list option , prompt is as below:

```
(00)extended            Extended Access List
```

```
(01)standard            Standard Access List
```

Please Input the code of command to be excute(0-1): 1

input 1 , Select standard option , prompt is as below:

```
(00)WORD                Standard Access-list name
```

Please Input the code of command to be excute(0-0): 0  
input 0.Select WORD option , prompt is as below:  
Please input a string:  
input list-name.

Step3 :

In the IP standard access list configuration Select 12 option , prompt is as below:

(00)any Any source host  
(01)A.B.C.D Address to match  
Please Input the code of command to be excute(0-1): 1  
input 1 , Select A.B.C.D option , prompt is as below:  
Please input a IP Address:

input source-address.

Since numerous different exists between IGMP-Router v1 and v3 on processing leave message, the upper configuration

| Step | Command                              | Purpose                            |
|------|--------------------------------------|------------------------------------|
| 1    | ip multicast ttl-threshold ttl-value | Configure TTL threshold on a port. |

command is invalid to IGMP-Router v1 and v3.

**Example of configuring IGMP Immediate-leave list**

The following example demonstrates the whole process of a system manager configuring the access list allowing “immediate leave” to be imme-leave on a port (ethernet 0/0 in the example) and adding an IGMP host address (192.168.20.168 in the example) into this access list. After these configuration steps, you can ensure that the IGMP host (IP is 192.168.20.168) has implemented “immediate leave” from multicast group.

```
interface ethernet 0/0
ip igmp immediate-leave imme-leave
exit
ip access-list standard imme-leave
permit 192.168.20.168
```

**Configure TTL Threshold**

You can use **ip multicast ttl-threshold** to configure TTL threshold the multicast message allowed to pass and use **ip (undo)multicast ttl-threshold** to apply default value. Default value is 1.

In the parameter prompt Select 17 option , prompt is as below:

(00)access-group Specify access control for packets  
.....  
(11)multicast Config ip multicast parameter  
.....  
Please Input the code of command to be excute(0-22): 11  
input 11 , Select multicast option , prompt:  
(00)boundary Config ip multicast boundary  
(01)helper-map Config ip multicast helper map  
(02)rate-limit Config ip multicast rate-limit term  
(03)ttl-threshold Config interface ttl threshold

Please Input the code of command to be excute(0-22): 3

input 3 , Select ttl-threshold option , prompt is as below:  
 (00)<0-255> ttl threshold  
 Please Input the code of command to be excute(0-22): 0  
 Select 0 , and specify ttl-value.

#### Example of TTL Threshold configuration

The following example demonstrates how to configure TTL threshold on a port.

```
interface ethernet 0/0
ip multicast ttl-threshold 200
```

#### Disable multicast fast forwarding

You can use to configure the port enabling multicast fast forwarding and use to disable this function:

| Step | Command         | Purpose                                       |
|------|-----------------|-----------------------------------------------|
| 1    | ip mroute-cache | Enable fast multicast forwarding on the port. |

In the parameter prompt select 17 option , prompt is as below:

```
(00)access-group          Specify access control for packets
.....
(9)mroute-cache          -- Forward multicast packet using mroute cache
.....
Please Input the code of command to be excute(0-22): 9
Select 9 option , confirm it.
```

#### Example of disable multicast fast forwarding

The following example demonstrates how to disable multicast fast forwarding on a port:

```
interface ethernet 0/0
no ip mroute-cache
```

#### Configure PIM-DM Task List

- Adjust timer
- Specify PIM-DM version
- Configure status refresh
- Configure filter list
- Configure DR priority
- Clear (S,G) imformation

#### Adjust Timer

The routing protocol employs several timerls to examine the frequency of sending hello messages and status refreshing. The interval size of sending hello message is concerned with whether the neighborhood can be correctly established.

To adjust timer, use the following command in router port configuration:

| Command                                      | Purpose                                                                                                                                                                                                        |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip pim-dm hello-interval                     | How long to send hello message to neighbors through the port.                                                                                                                                                  |
| ip pim-dm state-refresh origination-interval | As to the first hop router directly connected with source, it is the interval of periordically sending status refresh messages and only takes effect on configuring upward ports. As to the following routers, |

it is the interval of allowing receiving and processing the status refresh messages.

Take the first command for an example. :

In the parameter prompt select 17 option , prompt is as below:

(00)access-group Specify access control for packets

.....

(15)pim-dm PIM-DM interface commands

.....

Please Input the code of command to be excute(0-22): 15

input 15 , Select pim-dm option , prompt is as below:

(00)dr-priority PIM-DM router DR priority

(01)hello-interval PIM-DM router send hello interval

(02)state-refresh PIM-DM State-Refresh configuration

.....

Please Input the code of command to be excute(0-5): 1

input 1 , Select hello-interval option , configure the time.

Specify version

D-Link router PIM-DM only supports pim v2.

Because pim v1 has timed out, so we support pim v2 whether you have configured version or not. The purpose of this command is only to keep consistency with former style.

| Command                     | Purpose                                     |
|-----------------------------|---------------------------------------------|
| ip pim-dm version [version] | Configure PIM-DMversion on the router port. |

In the parameter prompt select 17 option , prompt is as below:

(00)access-group Specify access control for packets

.....

(15)pim-dm PIM-DM interface commands

.....

Please Input the code of command to be excute(0-22): 15

input 15 , Select pim-dm option , prompt is as below:

(00)dr-priority PIM-DM router DR priority

(01)hello-interval PIM-DM router send hello interval

(02)state-refresh PIM-DM State-Refresh configuration

(03)version PIM-DM version

.....

Please Input the code of command to be excute(0-5): 3

input 3 , Select version option .

Configur Status Refresh

In management directory, the default case will allow forwarding pim dense mode to refresh control message. Configuration command in port configure, as to first hop router directly connected with source, is the interval of sending refresh message periodically. Here it only effects on ascending ports. As it to back routers, it is the interval of the port allowing and processing status refresh message.

| Step | Command                                      | Purpose                                                                   |
|------|----------------------------------------------|---------------------------------------------------------------------------|
| 1    | ip(undo) pim-dm state-refresh disable        | Enable sending and receiving status refresh messages on the port.         |
| 2    | ip pim-dm state-refresh origination-interval | The interval of sending or receiving status refresh messages on the port. |

## Step1 :

In the parameter prompt select 17 option , first input U or u ,prompt is as below:

```
(00)access-group          Specify access control for packets
```

```
.....
```

```
(15)pim-dm                PIM-DM interface commands
```

```
.....
```

Please Input the code of command to be excute(0-22): 15

input 15 , Select pim-dm option , prompt is as below:

```
(00)dr-priority          PIM-DM router DR priority
```

```
(01)hello-interval      PIM-DM router send hello interval
```

```
(02)state-refresh       PIM-DM State-Refresh configuration
```

```
(03)version              PIM-DM version
```

```
.....
```

Please Input the code of command to be excute(0-5): 2

input 3 , Select state-refresh option , prompt is as below:

```
(00)origination-interval PIM-DM State-Refresh origination interval
```

Please Input the code of command to be excute(0-0): 0

input 0 , Select origination-interval option , prompt is as below:

```
(00)<4-100>             interval in seconds
```

```
(01)<cr>
```

Please Input the code of command to be excute(0-1):

Select parameter .

## Configure filter list

In default case PIM-DM has no filter lists. They are all configured in port configuration, including neighbour filter list and multicast bound filter list.

If you want to forbid a router or a network segment from adding in PIM-DM negotiation, you are required to configure neighbour filter list. To forbid or allow some groups passing this region, you should configure bound group filter list.

| Command                   | Purpose                         |
|---------------------------|---------------------------------|
| ip pim-dm neighbor-filter | Configure neighbor filter list. |
| ip multicast boundary     | Configure group filter list.    |

Take the first command for an example. :

In the parameter prompt select 17 option , prompt is as below:

```
(00)access-group          Specify access control for packets
```

```
.....
```

```
(15)pim-dm                PIM-DM interface commands
```

```
.....
```

Please Input the code of command to be excute(0-22): 15

input 15 , Select pim-dm option , prompt is as below:

```
(00)dr-priority          PIM-DM router DR priority
```

```
.....
```

```
(04)neighbor-filter      PIM-DM peering filter
```

```
.....
```

Please Input the code of command to be excute(0-5): 4

input 4 , Select neighbor-filter option , prompt is as below:

```
(00)WORD                IP Named Standard Access list
```

Please Input the code of command to be excute(0-0): 0

input 0 , Select WORD option , prompt is as below:  
 Please input a string:  
 input string.

Configure DR Priority

To be the same with IGMP v1, you should perform DR select ing. Router DR priority is 1 by default. When all PIM neighbor on the port support DR priority, the most prior become DR. If priorities are the same, the one has the maximum port ID become DR. If there are some routers no informing its priority in hello message, in case of many routers, the router has the maximum port ID become DR.

This command is performed in port configure:

| Command               | Purpose                                                   |
|-----------------------|-----------------------------------------------------------|
| ip pim-dm dr-priority | Configure local router DR priority on the specified port. |

In the parameter prompt select 17 option , prompt is as below:

```
(00)access-group          Specify access control for packets
.....
(15)pim-dm                PIM-DM interface commands
.....
```

Please Input the code of command to be excute(0-22): 15

input 15 , Select pim-dm option , prompt is as below:

```
(00)dr-priority          PIM-DM router DR priority
(01)hello-interval      PIM-DM router send hello interval
.....
```

Please Input the code of command to be excute(0-5): 0

input 0 , Select dr-priority option , prompt is as below:

```
(00)<0-4294967294>      DR priority
.....
```

Please Input the code of command to be excute(0-0): 0

input 0 , prompt is as below:

Please input a digital number:  
 input number.

Clear (S,G) information

In normal case, you may need to clear (S,G) item in local MRT or to clear the statistics of messages forwarded through (S,G) item. Use the following command in management directory:

| Command                                       | Purpose                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clear ip mroute pim-dm { *   group [source] } | Clear (S,G) item in local MRT. This operation will delete all or part of the items in local multicast routing table and maybe affect normal multicast forwarding. This command can only delete (S,G) items created by PIM-DM multicast routing protocol on upward ports. |
| clear ip pim-dm interface                     | Reset the multicast message statistics forwarded by (S,G) on PIM-DM port. This command can only reset (S,G) items created by PIM-DM multicast routing protocol on upward ports.                                                                                          |

Take the first command for an example. :

input clearCommand , prompt is as below:

```
(00)arp-cache          Clear the entire ARP cache
.....
(05)ip                 IP
.....
```

```

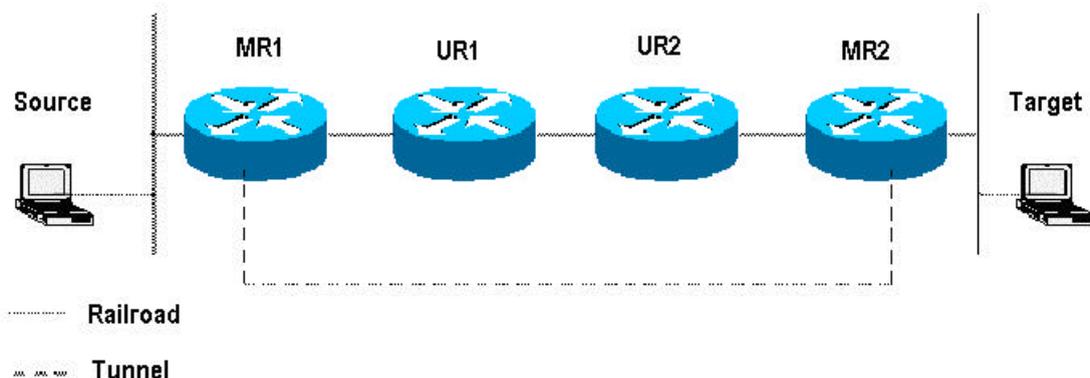
Please Input the code of command to be excute(0-15): 5
input 5 , Select ip option , prompt is as below:
(00)beigrp      Clear BEIGRP
      .....
(04)mroute      Delete multicast route table entries
      .....
Please Input the code of command to be excute(0-7): 4
input 4 , Select mroute option , prompt is as below:
(00)pim-dm     Clear PIM-DM MRT
Please Input the code of command to be excute(0-0): 0
input 0 , Select pim-dm option , prompt is as below:
(00)*          Delete all multicast routes
(01)A.B.C.D    IP group address
Please Input the code of command to be excute(0-1): 0
input 0 , confirm it.

```

### Configure multicast static route

Multicast static route allows multicast forwarding route differing from unicast route. RPF examination is processed when any multicast message is forwarded: The factual receiving port of the message is the one expected. (This port is the next hop of the unicast route of arriving at the sender.) Such examination is reasonable when unicast topology is the same with multicast topology. But in some cases we still wish the unicast route differ from multicast route.

A usual example is using tunnel technique. If a router on a route doesn't support multicast group protocol, the solution is configuring GRE tunnel between the two routers. In the following figure, each unicast router (UR) only supports unicast message and each multicast router (MR) supports multicast message. The source sends multicast messages to destination through MR1 and MR2. MR2 will forward a multicast message only when this message is received from tunnel. In this case, unicast messages from destination to source will also pass the tunnel. As we know, It is more slowly of sending messages on tunnel than sending directly.



Through configuring multicast static route, you can make the router process RPF examining according configuration instead of unicast routing table. So multicast messages employs tunnel and unicast messages do not. Multicast static route only resides in local and won't be advertised or process route forwarding.

Use the following command in global configure directory to configure multicast static route.

| Command                                                                       | Function                          |
|-------------------------------------------------------------------------------|-----------------------------------|
| <code>ip mroute source-address mask rpf-address type number[ distance]</code> | Configure multicast static route. |

input ip Command , prompt is as below:

```
(00)access-list      Named access-list
```

.....  
 (13)mroute                      Configure static multicast routes

.....  
 Please Input the code of command to be excute(0-25):        13  
 input 13 , Select option , prompt is as below:  
 (00)A.B.C.D      Source address  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select option , prompt is as below:  
 Please input a IP Address:  
 input address , prompt is as below:  
 (00)A.B.C.D      Network mask  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select option , prompt is as below:  
 Please input a IP Address:  
 input mask , prompt is as below:  
 (00)A.B.C.D      RPF neighbor address  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select option , prompt is as below:  
 Please input a IP Address:  
 input address , prompt is as below:  
 (00)interface-name  
 Please Input the code of command to be excute(0-0): 0  
 input 0 , Select option , prompt is as below:  
 Please input a interface name:  
 input name,prompt is as below:  
 (00)<0-255>      Administrative distance for mroute  
 (01)<cr>  
 Please Input the code of command to be excute(0-1):  
 Select parameter .

Control the transmission rate to IGMP group  
 Confiugre IP multicast boundary

Use **ip multicast boundary** to configure port multicast boundary. Use **ip(undo) multicast boundary** to cancel the boundary. The second configuring of this command will overlay the first configuring.

| Step | Command                           | Purpose                                      |
|------|-----------------------------------|----------------------------------------------|
| 1    | ip multicast boundary access-list | Configure IP multicast boundary on the port. |

In the parameter prompt select 17 option , prompt is as below:  
 (00)access-group                  Specify access control for packets  
 .....  
 (11)mcast                          Config ip multicast parameter  
 .....  
 Please Input the code of command to be excute(0-22): 11  
 input 11 , Select multicast option , prompt:  
 (00)boundary                      Config ip multicast boundary  
 (01)helper-map                    Config ip multicast helper map  
 (02)rate-limit                    Config ip multicast rate-limit term  
 (03)tll-threshold                 Config interface ttl threshold

Please Input the code of command to be excute(0-22): 0  
input 0 , Select boundary option , prompt is as below:  
(00)WORD      Access-list name  
Please Input the code of command to be excute(0-22): 0  
Select 0 option , then input access-list.

## Configure IP multicast flow control

Use **ip multicast rate-limit** to restrict the flow of multicast messages receiving or sending on a port in a range source/group. Use **no ip multicast rate-limit** to disable flow control.

Use the following command to configure input stream of a multicast flow to be n kbps:

| Step | Command                                                                                 | Purpose                                                                    |
|------|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| 1    | ip multicast rate-limit in<br>group-list access-list1<br>source-list access-list2 nkbps | Configure the maximum multicast inbound flow limit in a range on the port. |

In the parameter prompt select 17 option , prompt is as below:

```
(00)access-group      Specify access control for packets
.....
(11)mcast              Config ip multicast parameter
.....
```

Please Input the code of command to be excute(0-22): 11

input 11 , Select multicast option , prompt:

```
(00)boundary          Config ip multicast boundary
(01)helper-map        Config ip multicast helper map
(02)rate-limit        Config ip multicast rate-limit term
(03)tth-threshold     Config interface ttl threshold
```

Please Input the code of command to be excute(0-3): 2

input 2 , Select rate-limit option , prompt is as below:

```
(00)in                Broadcast Address
(01)out               IP Multicast Address
```

Please Input the code of command to be excute(0-1): 0

input 0 , Select in option , prompt is as below:

```
(00)<0-4294967>        Rate in kilobits per second
(01)group-list        IP Multicast Address
(02)source-list       Broadcast Address
(03)<cr>
```

Please Input the code of command to be excute(0-3): 1

input 1 , Select group-list option , prompt is as below:

```
(00)WORD              IP Standard Access List Name
```

Please Input the code of command to be excute(0-0): 0

Select 0 option , then input access-list1 , prompt is as below:

```
(00)<0-4294967>        Rate in kilobits per second
(01)source-list       Broadcast Address
(02)<cr>
```

Please Input the code of command to be excute(0-2): 1

input 1 , Select source-list option , prompt is as below:

```
(00)WORD    IP Standard Access List Name
Please Input the code of command to be excute(0-0): 0
Select 0 option , then input access-list2 , prompt:
(00)<0-4294967>      Rate in kilobits per second
(01)<cr>
Please Input the code of command to be excute(0-1):
Select option ,configure flow parameter .
```

Similarly you can configure output stream of a multicast flow to be n kbps:

| Step | Command                                                                                 | Purpose                                                            |
|------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| 1    | ip multicast rate-limit out<br>group-list access-list1<br>source-list access-list2 kbps | Configure the maximum multicast flow limit in a range on the port. |

### Configure IP multicast Helper

Use command ip multicast helper-map to configure connecting two broadcast network with multicast route in multicast network. Use ip (undo) multicast helper-map to cancel this command.

On the first hop router connected with source broadcast network:

| Step | Command                                                        | Purpose                                                                                         |
|------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| 1    | interface type number                                          | Enter into port configuration.                                                                  |
| 2    | ip multicast helper-map broadcast<br>group-address access-list | Configure command ip multicast helper and translate broadcast messages into multicast messages. |
| 3    | ip directed-broadcast                                          | Enable directed broadcast.                                                                      |
| 4    | ip forward-protocol [port]                                     | Configure the port number allowing forwarding messages.                                         |

#### Step1 :

input interface Command , prompt is as below:

```
(00)FastEthernet    FastEthernet interface
(01)Ethernet        Ethernet interface
.....
```

Please Input the code of command to be excute(0-10):

Select port type , prompt is as below:

Please input a interface name:

input port name.

#### Step2 :

In the parameter prompt select 17 option , prompt is as below:

```
(00)access-group    Specify access control for packets
.....
(11)multicast       Config ip multicast parameter
.....
```

Please Input the code of command to be excute(0-22): 11

input 11Select multicast option , prompt:

```
(00)boundary        Config ip multicast boundary
(01)helper-map      Config ip multicast helper map
```

```

(02)rate-limit          Config ip multicast rate-limit term
(03)tll-threshold      Config interface ttl threshold
    Please Input the code of command to be excute(0-3): 1
input 1 , Select helper-map option , prompt is as below:
(00)broadcast          Broadcast Address
(01)A.B.C.D            IP Multicast Address
Please Input the code of command to be excute(0-1): 0
Select 0 option , prompt is as below:
(00)A.B.C.D            IP Multicast Address or IP Broadcast Address
Please Input the code of command to be excute(0-0): 0
Select 0 option , prompt is as below:
Please input a IP Address:
input group-address , prompt is as below:
(00)WORD               Access-list name
Please Input the code of command to be excute(0-0): 0
Select 0 option , input access-list.

```

**Step3:**

In the prompt select 17 option , prompt is as below:

```

(00)access-group       Specify access control for packets
(01)address             IP address
(02)beigrp              Enhanced Interior Gateway Routing Protocol
(03)directed-broadcast Enable forwarding of directed broadcasts
    .....

```

Please Input the code of command to be excute(0-21): 3

input 3 , Select directed-broadcast option .

**Step4 :**

In global configure directory input ipCommand , prompt is as below:

```

(00)access-list        Named access-list
    .....
(09)forward-protocol   Controls forwarding of directed IP broadcasts
    .....

```

Please Input the code of command to be excute(0-25): 9

input 9 , Select forward-protocol option , prompt is as below:

```

(00)udp                Packets to a specific UDP port
Please Input the code of command to be excute(0-0): 0
input 0 , Select udp option , prompt is as below:
(00)<0-65535>          Port number
(01)biff                Biff (mail notification, comsat, 512)
(02)bootpc             Bootstrap Protocol (BOOTP) client (68)
    .....

```

Please Input the code of command to be excute(0-27):

Select port .

On the last hop router connected with destination broadcast network:

| Step | Command                               | Purpose                         |
|------|---------------------------------------|---------------------------------|
| 1    | interface type number                 | Enter into port configure mode. |
| 2    | ip directed-broadcast                 | Enable directed broadcast.      |
| 3    | ip multicast helper-map group-address | Configure command ip multicast  |

|   |                               |                                                                  |
|---|-------------------------------|------------------------------------------------------------------|
|   | broadcast-address access-list | helper and translate multicast messages into broadcast messages. |
| 4 | ip forward-protocol [port]    | Configure the port number allowing forwarding messages.          |

Step1 :

input interface Command , prompt is as below:

```
(00)FastEthernet      FastEthernet interface
(01)Ethernet          Ethernet interface
```

.....

Please Input the code of command to be excute(0-10):

Select port type , prompt is as below:

Please input a interface name:

input port name.

Step2:

In the prompt select 17 option , prompt is as below:

```
(00)access-group      Specify access control for packets
(01)address           IP address
(02)beigrp            Enhanced Interior Gateway Routing Protocol
(03)directed-broadcast Enable forwarding of directed broadcasts
```

.....

Please Input the code of command to be excute(0-21): 3

input 3 , Select directed-broadcast option .

Step3 :

In the parameter prompt select 17 option , prompt is as below:

```
(00)access-group      Specify access control for packets
.....
(11)multicast         Config ip multicast parameter
```

.....

Please Input the code of command to be excute(0-22): 11

input 11 , Select multicast option , prompt:

```
(00)boundary          Config ip multicast boundary
(01)helper-map        Config ip multicast helper map
(02)rate-limit        Config ip multicast rate-limit term
(03)ttl-threshold     Config interface ttl threshold
```

Please Input the code of command to be excute(0-3): 1

input 1 , Select helper-map option , prompt is as below:

```
(00)broadcast         Broadcast Address
(01)A.B.C.D           IP Multicast Address
```

Please Input the code of command to be excute(0-1): 1

Select 1 option , prompt is as below:

Please input a IP Address:

input group-address , prompt is as below:

```
(00)A.B.C.D           IP Multicast Address or IP Broadcast Address
```

Please Input the code of command to be excute(0-0): 0

Select 0 option , prompt is as below:

Please input a IP Address:

input broadcast-address , prompt is as below:

```
(00)WORD              Access-list name
```

Please Input the code of command to be excute(0-0): 0  
 Select 0 option , input access-list.

#### Step4 :

In global configure directory input ipCommand , prompt is as below:

```
(00)access-list      Named access-list
      .....
(09)forward-protocol Controls forwarding of directed IP broadcasts
```

Please Input the code of command to be excute(0-25): 9  
 input 9 , Select forward-protocol option , prompt is as below:

```
(00)udp      Packets to a specific UDP port
Please Input the code of command to be excute(0-0): 0
input 0 , Select udp option , prompt is as below:
(00)<0-65535> Port number
(01)biff      Biff (mail notification, comsat, 512)
(02)bootpc    Bootstrap Protocol (BOOTP) client (68)
```

.....  
 Please Input the code of command to be excute(0-27):  
 Select message port number.

#### Configure Stud multicast route

Use ip igmp helper-address and to ip pim-dm neighbor-filter configure Stud multicast route.  
 On the port connected with stud router and host:

| Step | Command                                       | Purpose                                                                          |
|------|-----------------------------------------------|----------------------------------------------------------------------------------|
| 1    | interface type number                         | Enter into port configuration.                                                   |
| 2    | ip igmp helper-address<br>destination-address | Configure ip igmp helper-address and relay multicast messages to central router. |

#### Step1 :

input interface Command , prompt is as below:

```
(00)FastEthernet    FastEthernet interface
(01)Ethernet        Ethernet interface
```

.....  
 Please Input the code of command to be excute(0-10):  
 Select port type , prompt is as below:  
 Please input a interface name:  
 input port name.

#### Step2:

In the prompt select 17 option , prompt is as below:

```
(00)access-group    Specify access control for packets
      .....
(06)igmp            IGMP interface command
```

.....  
 Please Input the code of command to be excute(0-21): 6  
 input 6 , Select igmp option , prompt is as below:  
 (00)helper-address relay igmp packet  
 (01)immediate-leave leave groups immediately without sending query

```
(02)join-group          IGMP join multicast group
.....
Please Input the code of command to be excute(0-8): 0
input 0 ,Select helper-address option ,prompt is as below:
(00)FastEthernet      FastEthernet interface
(01)Ethernet           Ethernet interface
(02)Serial             Serial interface
(03)Async              Asynchronous interface
(04)Null               Null interface
Please Input the code of command to be excute(0-4):
Select destination-address.
```

On the port connected with central router and stub router:

| Step | Command                                  | Purpose                                         |
|------|------------------------------------------|-------------------------------------------------|
| 1    | interface type number                    | Enter into port configuration.                  |
| 2    | ip pim-dm neighbor-filter<br>access-list | Filter all pim messages sent to stud<br>router. |

Step1 :

```
input interface Command ,prompt is as below:
(00)FastEthernet      FastEthernet interface
(01)Ethernet           Ethernet interface
.....
Please Input the code of command to be excute(0-10):
Select port type ,prompt is as below:
Please input a interface name:
input port name.
```

Step2:

```
In the prompt select 17 option ,prompt is as below:
(00)access-group      Specify access control for packets
.....
(15)pim-dm             PIM-DM interface commands
.....
Please Input the code of command to be excute(0-21): 15
input 15 ,Select pim-dm option ,prompt is as below:
(00)dr-priority        PIM-DM router DR priority
.....
(04)neighbor-filter   PIM-DM peering filter
.....
Please Input the code of command to be excute(0-5): 4
input 4 ,Select neighbor-filter option ,prompt is as below:
(00)WORD               IP Named Standard Access list
Please Input the code of command to be excute(0-0): 0
input 0 ,Select WORD option ,prompt ,
Please input a string:
input access-list.
```

Monitor and maintain multicast route

## Clear multicast buffer and routing table

If you consider a special buffer or routing table is invalidated, you can clear its content. Use this command in management directory:

| Command                                                                         | Function                                |
|---------------------------------------------------------------------------------|-----------------------------------------|
| <code>clear ip igmp group [type number]<br/>[group-address / &lt;cr&gt;]</code> | Clear items in IGMP cache.              |
| <code>clear ip mroute [* / group-address /<br/>source-address]</code>           | Clear items in multicast routing table. |

Take the first command for an example. :

input clear Command , prompt is as below:

(00)arp-cache            Clear the entire ARP cache

.....

(05)ip                    IP

.....

Please Input the code of command to be excute(0-15): 5

input 5 , Select ip option , prompt is as below:

(00)beigrp            Clear BEIGRP

.....

(03)igmp                IGMP clear commands

.....

Please Input the code of command to be excute(0-7): 3

input 3 , Select igmp option , prompt is as below:

(00)group                IGMP clear multicast-group commands

Please Input the code of command to be excute(0-0): 0

input 0 , Select group option , prompt is as below:

(00)interface-name

Please Input the code of command to be excute(0-0): 0

input 0 , Select interface-name option , prompt is as below:

Please input a interface name:f0/0

input port ,prompt is as below:

(00)A.B.C.D            IP group address

(01)<cr>

Please Input the code of command to be excute(0-1):

Select parameter .

## Show multicast routing table and system statistics

Through showing IP multicast routing table, concerned buffer or database, you can examine the source usage and resolve some network problems.

Use this command in management directory to observe the statistics about multicast route:

| Command                                                                     | Function                                     |
|-----------------------------------------------------------------------------|----------------------------------------------|
| <code>show ip igmp groups [type number  <br/>group-address] [detail]</code> | Display multicast information in IGMP group. |

|                                                                                     |                                                    |
|-------------------------------------------------------------------------------------|----------------------------------------------------|
| <code>show ip igmp interface [type number]</code>                                   | display IGMP configuration information on the port |
| <code>show ip mroute mfc</code>                                                     | display multicast forwarding cache.                |
| <code>show ip rpf [ucast   mstatic   pim-dm   pim-sm   dvmrp] source-address</code> | display RPF information                            |

Take the first command for an example. :

input show Command , prompt is as below:

```
(00)alias          alias for command
```

```
.....
```

```
(21)ip            IP information
```

```
.....
```

Please Input the code of command to be excute(0-49): 21

input 21 , Select ip option , prompt is as below:

```
(00)access-lists  List IP access lists
```

```
.....
```

```
(08)igmp          IGMP information
```

```
.....
```

Please Input the code of command to be excute(0-26): 8

input 8 , Select igmp option , prompt is as below:

```
(00)groups        IGMP group membership information
```

```
(01)interface     IGMP group membership information
```

Please Input the code of command to be excute(0-1): 0

input 0 , Select groups option , prompt is as below:

```
(00)A.B.C.D       IP group address
```

```
(01)interface-name
```

```
(02)detail        IGMPv3 source information
```

```
(03)<cr>
```

Please Input the code of command to be excute(0-3):

Select parameter .

Example of multicast route configuration

PIM-DM configure

This section contains example of PIM-DM configuration:

Basic PIM-DM configuration

A series-17 router, a cisco 2620. Configuration is as below:

Series-17 router configure:

```
!
ip multicast-routing
!
interface Null0
!
interface Loopback1
ip address 1.1.1.1 255.255.255.0
```

```
no ip directed-broadcast
ip pim-dm
ip igmp static-group *
!
interface Ethernet1/1
ip address 192.167.20.132 255.255.255.0
no ip directed-broadcast
duplex half
ip pim-dm
ip igmp static-group 239.1.1.1
!
!
interface Ethernet2/1
ip address 192.168.20.132 255.255.255.0
no ip directed-broadcast
duplex half
ip pim-dm
ip pim-dm neighbor-filter nbr_filter
!
!
ip access-list standard nbr_filter
deny 192.167.20.132 255.255.255.255
permit 192.168.20.0 255.255.255.0
!
Router B
interface ethernet 1/1
ip address 192.168.20.82 255.255.255.0
interface loopback 0
ip address 20.1.1.1 255.0.0.0
!
router PIM-DM
network 192.168.20.0
network 20.0.0.0
!
cisco 2620 configure:
!
ip multicast-routing
!
interface Loopback1
ip address 10.10.20.1 255.255.255.0
ip igmp static-group 239.1.1.1
ip pim dense-mode
!
interface FastEthernet0/0
ip address 192.168.20.204 255.255.255.0
ip pim dr-priority 20
ip pim query-interval 40
ip pim dense-mode
!
```

```
interface FastEthernet0/1
 ip address 192.168.20.204 255.255.255.0
 ip pim dr-priority 20
 ip pim query-interval 40
 ip pim dense-mode
```

!

Example of PIM-DM status refresh configuration

Refer to configure status refresh.

Example of administrative boundary configuration

The following example demonstrate how to configure administrative boundary of a port:

```
interface ethernet 0/0
 ip multicast boundary acl
```

```
ip access-list standard acl
 permit 192.168.20.97 255.255.255.0
```

Example of multicast Helper configuration

The following example demonstrates how to configure multicast helper.

Configuration on the router is as below: Configure ip directed-broadcast on port e0 of the first hop router to allow direct broadcast message processing. Configure ip multicast helper-map broadcast 230.0.0.1 testacl1 to allow translating udp broadcast messages whose port number is 4000 and sent by source address 192.168.20.97/24 into multicast messages whose destination address is 230.0.0.1 for transmitting.

Configure ip directed-broadcast on port e1 of the last hop router to allow direct broadcast message processing. Configure **ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2** to allow translating udp multicast messages whose port number is 4000, destination is 230.0.0.1 and sent by source address 192.168.20.97/24 into broadcast messages whose destination address is 172.10.255.255 for transmitting.

On the first hop router connected with source broadcast network:

```
interface ethernet 0
 ip directed-broadcast
 ip multicast helper-map broadcast 230.0.0.1 testacl1
 ip pim-dm
 !
 ip access-list extended testacl1 permit udp 192.168.20.97 255.255.255.0 any
 ip forward-protocol udp 4000
```

On the last hop router connected with destination broadcast network:

```
interface ethernet 1
 ip directed-broadcast
 ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
 ip pim-dm
 !
 ip access-list extended testacl2 permit udp 192.168.20.97 255.255.255.0 any
 ip forward-protocol udp 4000
```

Example of Stub multicast configuration

Configuration of router A and B are as below:

## Stub Router A Configuration

```
ip multicast-routing
ip pim-dm
ip igmp helper-address 10.0.0.2
```

## Central Router B Configuration

```
ip multicast-routing
ip pim-dm
ip pim-dm neighbor-filter stubfilter
```

```
ip access-list stubfilter
  deny 10.0.0.1
```

## 6. Security Configuration

In this chapter we will introduce our company's network security solution to you. If you desire to improve your network security strategy, this chapter will provide an ideal answer for you. Also we will introduce how to configure an authentication, authorization, recording, and relating TACACS+ and the configuration methods of RADIUS. Meanwhile, you will learn the usage methods of IPSec.

### 6.1 Configure AAA

#### 6.1.1 AAA Overview

Access Control is to control the users have access to Router or Network Access Server (NAS), and limit the service types that can be used by them. This feature provides Authentication, Authorization, Accounting (AAA) functions so as to improve the network security.

##### 6.1.1.1 AAA Security Service

Authentication is the way to identify the users before accepting their requests for access and network service. You can define a named list of authentication methods to configure the AAA authentication, and then apply this list on each port. The list has defined the authentication methods that have been executed and their execution order; any defined authentication method must be applied on a specific port before it is executed. The only exception is the list of default methods( named "default"). If there's no other methods lists, the default will be automatically applied to all ports. Definition of any method list will cover the default. As for detailed information of all authentication configuration methods, please refer to [Authentication Configuration](#).

Authorization——Provide a method for remote access control, used to limit the user's service priority.

AAA authorize a user to function through a group of properties regarding this user, and these properties describe which priorities have been given to the user. Router compares these properties with the specific user information that is included in the database and reply the result to AAA, so as to determine the actual priority of the this user. This database locates in the local server that is been accessing or Router, or in a remote RADIUS or TACACS+ security server. The user is authorized through the Attribute-Value Pairs, defining priorities that are allowed to authorize and relating to the user. All authorization methods must be according to the AAA definition. Similar to authentication, first of all, you shall have to define a list of authorized methods, and apply this list to all ports. As for detailed information of AAA authorization configuration, please refer to "Authorization Configuration".

Accounting——Provides a method for collecting user service information and sending it to the security server. This info can be used to offer an account, audit and form a report form, such as user identifier, start and end time, executed command, the number of packets and bytes.

Accounting traces not only the users' access service, but also the network resource that they consumed. Once enable the AAA accounting feature, the network access server will report the user's activities to the TACACS+ or RADIUS security server in the form of accounting. Each piece of accounting, including accounted Attribute-Value pairs, is stored on the security server. These data can used for network management, customer bill or audit analysis. Alike the authentication and authorization, you shall have to define a list of accounting methods, and apply this list to all ports. As for detailed information of AAA accounting configuration, please refer to "Accounting Configuration".

AAA is a system structure that uses the same configuration method to configure three independent security functions, which provides modularized methods to complete the following service:

Authentication——Provides a method to identify the user, incl. enquiry of user name and password, and encryption in accordance with the selected security protocol.

##### 6.1.1.1.1 Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control
- Easy to update
- Standardized authentication methods, such as RADIUS and TACACS+

- Multiple backup systems

### 6.1.1.1.2 Basic Theories Of AAA

AAA is designed to dynamically configure the types of authentication and authorization based on each line (user) or service (eg. IP, IPX or VPDN). You can define the authentication and authorization types by creating method lists and then apply these lists on a specific service or port.

### 6.1.1.1.3 List Of Methods

The list of authentication methods defines multiple methods used to authenticate a user. The administrator can configure one or more protocols used for authentication in the method list, therefore, to ensure that you can have a backup authentication method in case the former method fails. Firstly, list one method, if it doesn't work out any response, please select the second method on the methods list; This process will continue until the listed method successfully carries out an authentication or use up the resource of authentication method list, in this case, the authentication turns out to be fail.

**Note: The later methods to attempt authentication are only used when the former ones don't work. As long as any part of this authentication process fails—in other words, the response from the security server or local user names database is to reject the user to access—the authentication process ends, and there will be no more attempt to proceed.**

Figure 1 shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers.

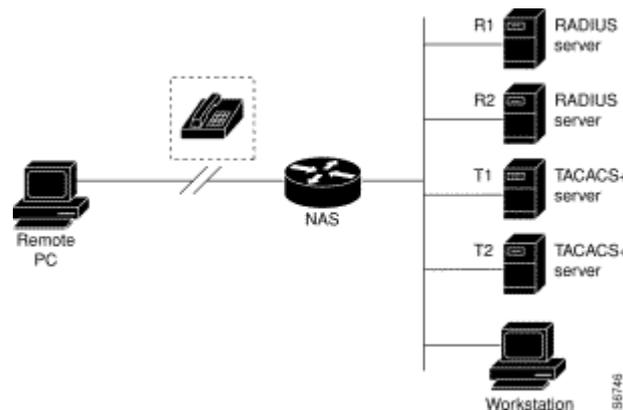


Figure 1

Suppose the system administrator has determined that all ports authenticate the PPP based connection with the same authentication method in the security scheme: Firstly, connect R1 to learn the relating authentication information, if R1 doesn't respond, then connect R2, if R2 doesn't respond, then T1, then T2. If all designated server don't respond, the authentication will be focused on the local user name database of the access server itself. When a remote user is attempting to access the network by dial-up, the network server will demand the relative authentication info on R1, if the user is authenticated to be legal, it will send a PASS reply to network access server, to enable the user to access the server; If R1 answers FAIL message, the user will be turned down, the session terminated. If there's no response from R1, the network server will view it as a ERROR and try to find the authentication info on R2. This model will last in the rest of the time until the user is accepted or rejected, or the termination of this session.

**Note: Please remember that a FAIL response completely differs from an ERROR response. FAIL indicates that the user has not met the criteria of a successful authentication that contained in the authentication database, and the authentication ends up with a FAIL response. ERROR means that the security server has not responded to an authentication query. Only if AAA detected ERROR will it choose the next authentication method defined in the authentication methods list.**

### 6.1.1.2 Configuration Process

Firstly, decide which kind of security solution you want to have. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack.

#### 6.1.1.2.1 Overview of the AAA Configuration Process

Configuring AAA is relatively simple after understanding the basic process involved. To configure security on a our router or access server with AAA, please follow the following steps:

- If you decide to use a security server, configure security protocol parameters, such as RADIUS, TACACS+.
- Define the method lists for authentication using **aaa authentication** command.
- Apply the method lists to a particular interface or line, if necessary.

#### 6.1.1.2.2 Configure Task Related Files

Table 1 explains AAA configuration task and where to find more information.

| Further Configuration Tasks                                    | Reference Information                       |
|----------------------------------------------------------------|---------------------------------------------|
| Configure Local Login Authentication                           | <a href="#">Authenticaton Configuration</a> |
| Using the security servers to control the login authentication | <a href="#">Authenticaton Configuration</a> |
| Defining the method lists applied to authentication            | <a href="#">Authenticaton Configuration</a> |
| applying the lists to the particular interface or line         | <a href="#">Authenticaton Configuration</a> |
| configure the parameters of RADIUS protocol                    | <a href="#">Configure RADIUS</a>            |
| configure the parameters of TACACS+ protocol                   | <a href="#">Configure TACACS+</a>           |

Table1: Tasks and Documents

### 6.1.2.1 List of AAA Authentication Methods

Authentication identifies users before they are allowed access to the network.

#### 6.1.2.1.1 Examples Of Methods List

To configure AAA authentication, first of all, define a named list of authentication methods, and then apply that list to different interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which, by coincidence, is named “default”). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is for describing the authentication methods to be queried, in sequence, to authenticate a user. Method lists enable you to designate one or more security protocols used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Our Router uses the first method listed to authenticate users; if that method fails to respond, the Router selects the next authentication method listed in the method list. This process lasts until one of the listed methods is successfully authenticated or the use up of all the methods.

It is important to note that the Router initiates an attempt to authenticate with a method listed behind only when the previous method doesn't work out any response. If authentication fails at any part of this process—meaning that the security server or local username database responds by denying the user access—the authentication process terminates and there will be no more authentication attempt.

#### 6.1.2.1.1 Examples Of Methods List

Figure 1 shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers.

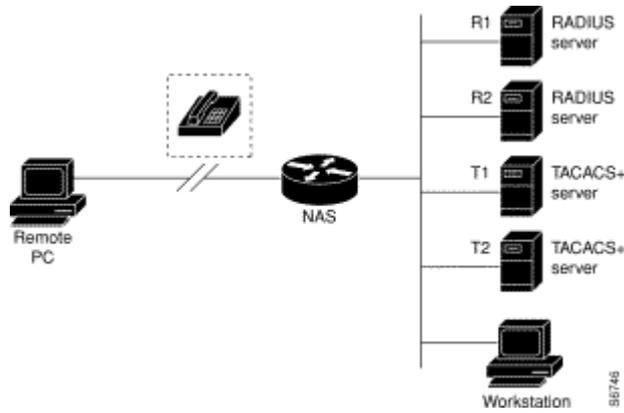


Figure 1

Suppose the system administrator has determined that all ports authenticate the PPP based connection with the same authentication method in the security scheme: Firstly, connect R1 to learn the relating authentication information, if R1 doesn't respond, then connect R2, if R2 doesn't respond, then T1, then T2. If all designated server don't respond, the authentication will be focused on the local user name database of the access server itself. In order to realize this, the system admin needs to input the following command: `aaa (default) authentication ppp radius local`.

In this example, "default" is the name of the method list. The protocols included in this method list are listed after the name, in the order they are to be queried. The default list is automatically applied to all interfaces.

When a remote user is attempting to access the network by dial-up, the network server will demand the relative authentication info on R1, if the user is authenticated to be legal, it will send a PASS reply to network access server, to enable the user to access the server; If R1 answers FAIL message, the user will be turned down, the session terminated. If there's no response from R1, the network server will view it as a ERROR and try to find the authentication info on R2. This model will last in the rest of the time until the user is accepted or rejected, or the termination of this session.

It is important to remember that a FAIL response completely differs from an ERROR response. FAIL indicates that the user has not met the criteria of a successful authentication that contained in the authentication database, and the authentication ends up with a FAIL response. ERROR means that the security server has not responded to an authentication query. Only if AAA detected ERROR will it choose the next authentication method defined in the authentication methods list.

Suppose that the system administrator wants to apply a methods list only on a particular interface or set of interfaces. In this case, the system admin needs to create a non-default named methods list and apply this list to an appropriate port. This example below indicates how a system admin implements a certain authentication method only on an asynchrony port:

```
[DEFAULT@RouterA /config/]#aaa
(00)accounting           Accounting configurations parameters
(01)authentication      Authentication configurations parameters
.....
Please Input the code of command to be excute(0-5): 1
.....
(03)ppp                 Set authentication list for ppp
(04)username-prompt     Text to use when prompting for a username
Please Input the code of command to be excute(0-4): 3
(00)WORD                Named authentication list
(01)default              The default authentication list.
```

```

Please Input the code of command to be excute(0-1): 1
.....
(05)radius                               Use all radius server for authentication
(06)tacacs+                               Use all tacacs+ server for authentication
Please Input the code of command to be excute(0-6): 5
(00)group                                 Use Server-group
(01)group-restrict                        If user has specified a server,this group will not be used
(02)local                                 Use local username authentication
.....
Please Input the code of command to be excute(0-6): 2
.....
(03)tacacs+                               Use all tacacs+ server for authentication
(04)<cr>
Please Input the code of command to be excute(0-4): 4
Will you excute it? (Y/N):y
[DEFAULT@RouterA /config/]#aaa
(00)accounting                            Accounting configurations parameters
(01)authentication                        Authentication configurations parameters
.....
Please Input the code of command to be excute(0-5): 1
.....
(03)ppp                                  Set authentication list for ppp
(04)username-prompt                       Text to use when prompting for a username
Please Input the code of command to be excute(0-4): 3
(00)WORD                                  Named authentication list
(01)default                               The default authentication list.
Please Input the code of command to be excute(0-1): 0
Please input a string:async0 (输入 authentication list name , 此处仅为示例)
.....
(05)radius                               Use all radius server for authentication
(06)tacacs+                               Use all tacacs+ server for authentication
Please Input the code of command to be excute(0-6): 5
.....
(05)tacacs+                               Use all tacacs+ server for authentication
(06)<cr>
Please Input the code of command to be excute(0-6): 5
(00)group                                 Use Server-group
(01)group-restrict                        If user has specified a server,this group will not
be used
(02)local                                 Use local username authentication
.....
Please Input the code of command to be excute(0-5): 2
(00)group                                 Use Server-group
(01)group-restrict                        If user has specified a server,this group will not be used
(02)none                                  NO authentication
(03)<cr>
Please Input the code of command to be excute(0-3): 2
(00)<cr>
Please Input the code of command to be excute(0-0): 0

```

```

Will you excute it? (Y/N):y

[DEFAULT@RouterA /config/]#interface
(00)FastEthernet          FastEthernet interface
(01)Serial                Serial interface
(02)Async                 Asynchronous interface
.....
Please Input the code of command to be excute(0-9): 2
Please input a interface name:a0/0 (输入端口名称, 此处仅为示例)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(27)ppp                  Point-to-point protocol
(28)priority-group      Assign a priority group to interface
.....
Please Input the code of command to be excute(0-35): 27
Key Word:
  U(undo) D(default)    Q(quit)
(00)authentication     Set PPP link authentication method
(01)authorization      Set PPP network authorization method
.....
Please Input the code of command to be excute(0-9): 0
(00)chap               Challenge Handshake Authentication Protocol (CHAP)
(01)ms-chap            Microsoft Challenge Handshake Authentication
Protocol (MS-CHAP)
(02)pap                Password Authentication Protocol (PAP)
Please Input the code of command to be excute(0-2): 0
(00)WORD               Use an authentication list with this name
(01)callin             Authenticate remote on incoming call only
.....
Please Input the code of command to be excute(0-5): 0
Please input a string:async0 (Input the same authentication list name with the above)
Will you excute it? (Y/N):y

```

In this example, “async0” is the name of the method list, and the protocols included in this method list are listed after the name in the order in which they are to be performed. After the creation of method list, the list will be applied on the appropriate port. Note that the method list name in a **aaa authentication** command must match that in the **ppp authentication** command.

### 6.1.2.2 General Configuration Process of AAA Authentication

To configure AAA authentication, you need to finish the following configuration process:

If you are using a security server, please configure the security protocol parameters, like RADIUS and TACACS.

Define the authentication methods list with **aaa authentication** command.

Apply the methods list to a specific port or line if necessary.

### 6.1.2.3 AAA Authentication Methods Description

## 6.1.2.3.1 Use AAAConfiguration Login Authentication

The AAA security service facilitates a variety of login authentication methods. You will have to start AAA authentication with **aaa authentication** command using whatever login method. Create one or more lists of authentication methods in **aaa authentication login** command, used in login. These lists are applied with the circuit configuration command **login authentication**. When configuring, please use the commands below, starting from the global configuration directory:

| Step | Command                                                                      | Purpose                                            |
|------|------------------------------------------------------------------------------|----------------------------------------------------|
| 1    | <b>aaa (default) authentication login</b> {list-name}method1<br>[method2...] | Create a global authentication list                |
| 2    | <b>line</b> [aux   console   tty   vty] line-number<br>[ending-line-number]  | Enter the config mode of a certain line            |
| 3    | <b>login (default) authentication</b> {list-name}                            | Apply the authentication list to one or more lines |

```
[DEFAULT@RouterA /config/]#aaa
(00)accounting                Accounting configurations parameters
(01)authentication            Authentication configurations parameters
.....
Please Input the code of command to be excute(0-5): 1
(00)enable                    Set authentication list for enable
(01)login                     Set authentication list for login
.....
Please Input the code of command to be excute(0-4): 1
(00)WORD                      Named authentication list
(01)default                   The default authentication list.
Please Input the code of command to be excute(0-1): 0
Please input a string:list1 (Input authentication list name ,this is only for example)
(00)enable                    Use enable password for authentication
(01)group                     Use Server-group
(02)group-restrict            If user has specified a server,this group will not
be used
(03)line                      Use line password for authentication
(04)local                     Use local username authentication
.....
Please Input the code of command to be excute(0-8): 4
.....
(05)tacacs+                   Use all tacacs+ server for authentication
(06)<cr>
Please Input the code of command to be excute(0-6): 6
Will you excute it? (Y/N):y
[DEFAULT@Router /config/]#line
Key Word:
U(undo) D(default)          Q(quit)
(00)aux                      Auxiliary line
(01)console                  Primary terminal line
(02)tty                     Terminal controller
(03)vty                     Virtual terminal
```

```

Please Input the code of command to be excute(0-3): 3
Key Word:
Q(quit)
(00)<0-63>                               First Line number
Please Input the code of command to be excute(0-0): 0
Please input a digital number:1 (Input First Line number)
Key Word:
Q(quit)
(00)<2-63>                               Last Line number
(01)<cr>
Please Input the code of command to be excute(0-1): 0
Please input a digital number:63 (Input FLast Line number)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(18)login                               Login AAA settings
(19)monitor                             Copy debug output to the current terminal line
.....
Please Input the code of command to be excute(0-36): 18
Key Word:
U(undo)  D(default)      Q(quit)
(00)authentication      Line login authentication parameters
(01)authorizatn         Line login authorizatn parameters
(02)accounting          Line login accounting parameters
Please Input the code of command to be excute(0-2): 0
Key Word:
Q(quit)
(00)WORD                Authentication list name
(01)default             Use the default authentication list
Please Input the code of command to be excute(0-1): 0
Please input a string:lista (Input Authentication list name)
Will you excute it? (Y/N):y

```

The keyword “list-name” is to name any string of a created list. The keyword “method” defines the actual method that used in an authentication process. If only the former method returns to the authentication error, other methods will then be used; If the former methods turns out to be failed, there will be no more attempt to authenticate with other methods. If you want to designate to launch a successful login even if all methods have returned to authentication erro, simply specify “none” in the command line as the last authentication method. For instance, Even if the TACACS+ service has returned to error, the authentication can still succeed, using the following command:

```
aaa (default) authentication login tacacs+ none
```

You can setup a default list with default parameters. The default list is automatically applied to all interfaces. For instance, you can use the following command when designating RADIUS as the default authentication method for users to login:

```
aaa (default) authentication login radius
```

**Note: Since the keyword none enables any uesr that has logged in to successfully pass the authentication, you shall have to keep this keyword as the backup method.**

Following table lists the currently supported login authentication methods.

| Key Word       | Description                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------|
| enable         | Use enable password to authenticate                                                                           |
| group          | Use a server group to authenticate                                                                            |
| group-restrict | Use a server group to authenticate, but when a user has specified some server, this group will be invalidated |
| line           | Use a line password to authenticate                                                                           |
| local          | Use a local database to authenticate                                                                          |
| local-case     | Use a local database to authenticate(the user name is case-sensitive)                                         |
| none           | The authentication can pass unconditionally                                                                   |
| radius         | Use RADIUS authentication                                                                                     |
| tacacs+        | Use TACACS+ authentication                                                                                    |

#### ■ ? Login Authentication With Enable Password

Use the **aaa authentication login** command with the **enable** *method* keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter:

```
aaa (default) authentication login enable
```

#### ■ ? Login Authentication Using Line Password

Use the **aaa authentication login** command with the **line** *method* keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following:

```
aaa (default) authentication login line
```

Before you can use a line password as the login authentication method, you need to define a line password.

#### ■ ? Login Authentication Using Local Password

Use the **aaa authentication login** command with the **local** *method* keyword to specify that the local username database will be used as the login authentication method. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following:

```
aaa (default) authentication login local
```

For information about adding users into the local username database, see the [“Establish Local Authentication Database”](#) section in this chapter.

#### ? Login Authentication Using RADIUS

Use the **aaa authentication login** command with the **radius** *method* keyword to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following:

```
aaa (default) authentication login radius
```

Before you can use RADIUS as the login authentication method, you need to configure the RADIUS service. For more information, refer to the [“Configuring RADIUS”](#) chapter.

## ■ ? Login Authentication Using TACACS+

Use the **aaa authentication login** command with the **tacacs+ method** keyword to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa (default) authentication login tacacs+
```

Before you can use TACACS+ as the login authentication method, you need to configure TACACS+ service. For more information, refer to the “[Configuring TACACS+](#)” chapter.

### 6.1.2.3.2 Use AAA To Proceed PPP Authentication

Many users access network access servers through dialup via async or ISDN. The AAA security services facilitate a variety of authentication methods for use on serial interfaces running PPP. Use the **config-aaa authentication ppp** command to start AAA authentication no matter which of the supported PPP authentication methods you decide to use. To configure AAA authentication methods for serial lines using PPP, use the following commands in global configuration directory:

| Step | Command                                                                                     | Purpose                                                                                                  |
|------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| 1    | <b>aaa (default) authentication ppp</b> {list-name}<br><i>method1</i> [ <i>method2...</i> ] | Create a local authentication list.                                                                      |
| 2    | <b>interface</b> interface-type number                                                      | Enter interface configuration mode for the interface to which you want to apply the authentication list. |
| 3    | <b>ppp (default) authentication</b> {chap   pap   chap pap   pap chap} {list-name}          | Apply the authentication list to a line or set of lines.                                                 |

Example :

1. Create a very low authentication list :

```
[DEFAULT@Router /config/#aaa
(00)accounting Accounting configurations parameters
(01)authentication Authentication configurations parameters
.....
Please Input the code of command to be excute(0-5): 1
.....
(03)ppp Set authentication list for ppp
(04)username-prompt Text to use when prompting for a username
Please Input the code of command to be excute(0-4): 3
(00)WORD Named authentication list
(01)default The default authentication list.
Please Input the code of command to be excute(0-1): 0
Please input a string:bdcom (input authentication list)
(00)group Use Server-group
(01)group-restrict If user has specified a server,this group will not be used
(02)local Use local username authentication
.....
Please Input the code of command to be excute(0-6): 2
.....
(03)radius Use all radius server for authentication
```

```

(04)tacacs+                               Use all tacacs+ server for authentication
(05)<cr>
Please Input the code of command to be excute(0-5): 3
.....
(03)tacacs+                               Use all tacacs+ server for authentication
(04)<cr>
Please Input the code of command to be excute(0-4): 4
Will you excute it? (Y/N):y

[DEFAULT@Router /config/]#interface
(00)FastEthernet                          FastEthernet interface
(01)Serial                                 Serial interface
.....
Please Input the code of command to be excute(0-9): 1
Please input a interface name:s0/1 (input the port name)
Will you excute it? (Y/N):y
Key Word:
  Q(quit)
.....
(25)physical-layer                       Configure physical layer parameters
(26)ppp                                   Point-to-point protocol
.....
Please Input the code of command to be excute(0-34): 26
Key Word:
  U(undo)      D(default)      Q(quit)
(00)authentication          Set PPP link authentication method
(01)authorization          Set PPP network authorization method
(02)callback                Set CALLBACK parameters
.....
Please Input the code of command to be excute(0-9): 0
(00)chap                    Challenge Handshake Authentication Protocol (CHAP)
(01)ms-chap                 Microsoft Challenge Handshake Authentication
Protocol (MS-CHAP)
(02)pap                     Password Authentication Protocol (PAP)
Please Input the code of command to be excute(0-2): 0
(00)WORD                    Use an authentication list with this name
(01)callin                  Authenticate remote on incoming call only
.....
Please Input the code of command to be excute(0-5): 0
Please input a string:bdcom (input authentication list name)
Will you excute it? (Y/N):y

```

With **aaa authentication ppp** command, you can create one or more lists of authentication methods that are used when a user begins to run PPP. These lists are applied using the **ppp authentication** line configuration command. To create a default list, use the **default** parameter followed by the methods you want used in default situations. For example, to specify the local username database as the default method for user authentication, enter the following:

```
aaa (default) authentication ppp local
```

The keyword *list-name* is any character string used to name the list you are creating. The keyword *method* refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line. For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command line:

```
aaa (default) authentication ppp local
```

Keyword *list-name* is to name any string in a created list. Keyword *method* is to designate the actual method that is adopted during the authentication. If only the previous methods return to authentication error, will other methods be used; If the previous methods return to authentication failure, will there be no more method to authenticate. If you want to specify that even all methods returned to error can still successfully carry on the authentication, you should simply specify *none* as the last authentication method in the command line. For instance, in the following example, if you want to ensure the successful authentication even if the TACACS + server returns error, you can input the command line of:

```
aaa (default) authentication ppp tacacs+ none
```

**Note: Since *none* allows all users logging in to authenticate successfully, it should be used as a backup method of authentication.**

Following table lists the AAA authentication PPP methods:

| Keyword               | Description                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>group</b>          | Use a server group to authenticate                                                                                  |
| <b>group-restrict</b> | Use a server group to authenticate, but when a user has designated a certain server, this group will be invalidated |
| <b>local</b>          | Use the local username database to authenticate                                                                     |
| <b>local-case</b>     | Use the local username database to authenticate(the username is case-sensitive)                                     |
| <b>none</b>           | The authentication will pass unconditionally                                                                        |
| <b>radius</b>         | Use RADIUS authentication                                                                                           |
| <b>tacacs+</b>        | Use TACACS+ authentication                                                                                          |

#### ■ ? PPP Authentication Using Local Password

In *aaa authentication ppp* command, the keyword *local* is used to designate to authenticate with a local username database. For instance, if you want to designate the local username database as the authentication method on a PPP line without using other methods, you can input the following command line:

```
aaa (default) authentication ppp local
```

For information about adding users into the local username database, see the “[Establish Local AuthenticationDatabase](#)” section in this chapter.

#### ■ ? PPP Authentication Using RADIUS

In *aaa authentication ppp* command, the keyword RADIUS is used to designate RADIUS to authenticate. For instance, if you want to designate the local username database as the authentication method on a PPP line without using other methods, you can input the following command line:

```
aaa (default) authentication ppp radius
```

While use RADIUS as the authentication method, you need to configure the RADIUS service. For more information, refer to the “Configure RADIUS” chapter.

■ ? PPP Authentication Using TACACS+

Use the *config-aaa authentication ppp* command with the keyword TACACS+ to specify TACACS+ as the authentication method for use on interfaces running PPP. For example, to specify TACACS+ as the method of user authentication when no other method list has been defined, enter the following:

```
aaa (default) authentication ppp tacacs+
```

Before use TACACS+ as the authentication method, you need to enable communication with the TACACS+ service. For more information, refer to the “Configure TACACS+” chapter.

6.1.2.3.3 Initiate Password Protection When Enter A Priority Level

Use the *config-aaa authentication enable default* command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication succeed even if all methods return an error, specify **none** as the final method in the command line. Use the following command in global configuration mode:

| Command                                                                     | Purpose                                                                     |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| aaa (default) authentication enable <i>method1</i><br>[ <i>method2...</i> ] | Initiate password authentication when a user is entering the priority level |

```
[DEFAULT@Router /config/]#aaa
(00)accounting Accounting configurations parameters
(01)authentication Authentication configurations parameters
.....
Please Input the code of command to be excute(0-5): 1
(00)enable Set authentication list for enable
(01)login Set authentication list for login
.....
Please Input the code of command to be excute(0-4): 0
(00)default The default authentication list.
Please Input the code of command to be excute(0-0): 0
(00)enable Use enable password for authentication
(01)line Use line password for authentication
(02)none NO authentication
Please Input the code of command to be excute(0-2): 1
(00)enable Use enable password for authentication
(01)none NO authentication
(02)<cr>
Please Input the code of command to be excute(0-2): 2
Will you excute it? (Y/N):y
```

The keyword *method* refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

Following table lists the supported login authentication methods:

| Keyword               | Description                                                                                                      |
|-----------------------|------------------------------------------------------------------------------------------------------------------|
| <b>enable</b>         | Use enable password for authentication                                                                           |
| <b>group</b>          | Use server group for authentication                                                                              |
| <b>group-restrict</b> | Uses the list of all servers for authentication, but when using the specified server, the group will be invalid. |
| <b>line</b>           | Uses the line password for authentication.                                                                       |
| <b>none</b>           | Uses no authentication.                                                                                          |
| <b>radius</b>         | Uses RADIUS authentication.                                                                                      |
| <b>tacacs+</b>        | Uses TACACS+ authentication.                                                                                     |

When configured *enable* authentication method as the remote authentication (i.e. configured *group*, *group-restrict*, *radius* or *tacacs+* as the keywords), the usernames that respectively use RADIUS and TACACS+ to authenticate are different, the following is the introduction for each type:

- Use RADIUS to proceed enable authentication:

The authenticated username is \$ENABLE*level*\$, in which *leve* indicates the privilege level that the user is to enter, i.e. the number that implies the privilege number behind enable command. For instance, if you are to enter a privilege level 7, you needs to input command enable 7. In this case, if you has configured to use RADIUS for authentication, then the username submitted to Radius server is \$ENABLE15\$, thus need to configure relating username and password on Radius server in advance. It is especially pointed out that you need to clarify that the service type used for privilege authentication in the Radius Server user database is 6, i.e. Admin-User .

- Use TACACS+ to proceed authentication

The username used for enable authentication is the one that used when this user login the Router. For example, if a user typedchen for username when login in the Router, the username used for enable authentication should be chen too. If the user is not required to pass authentication or is not indicated to input the username when proceeding the authentication, the username after successful login should be DEFAULT, and you need to set up in the user database of TACACS+ Server.

#### 6.1.2.3.4 Change The String To Prompt Inputting The Password

Use **aaa authentication password-prompt** command to change the default text that the D-Link router displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **undo** form of this command restores the password prompt to the following default value:

Password :

**aaa authentication password-prompt** command does not change any prompt message provided by a remote TACACS+ server or RADIUS server. Use the following command in global configuration directory:

| Command                                                      | Purpose                                                                        |
|--------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>aaa authentication password-prompt</b> <i>text-string</i> | Change the default text displayed when a user is prompted to enter a password. |

#### Example:

```
[DEFAULT@Router /config/]#aaa
```

```
(00)accounting           Accounting configurations parameters
(01)authentication       Authentication configurations parameters
```

```

.....
Please Input the code of command to be excute(0-5): 1
(00)enable                Set authentication list for enable
(01)login                 Set authentication list for login
(02)password-prompt      Text to use when prompting for a password
.....
Please Input the code of command to be excute(0-4): 2
(00)WORD                 Password prompt string
Please Input the code of command to be excute(0-0): 0
Please input a string:123456 ( Input password -prompt , here is only for example )
Will you excute it? (Y/N):y

```

### 6.1.2.3.5 Establish A Database of Local User Name Authentication

A local authentication system based on the username can be created for the following situations:

- To provide a TACACS-like username and encrypted password-authentication system for networks that cannot support TACACS
- To provide special-case logins: such as, access list verification, no password verification, autocommand execution at login.

To establish the local authentication database, perform the following command in the global configuration mode:

| Command                                                                                 | Purpose     |
|-----------------------------------------------------------------------------------------|-------------|
| <code>username name password { password   [encryption-type] encrypted-password }</code> | 建立用户名及对应的密码 |

Example:

```

[DEFAULT@Router /config/]#username
(00)WORD                User name
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom (Input username , here is only for example)
.....
(04)nocallback-verify  Do not require authentication after callback
(05)password           Specify the password for the user
.....
Please Input the code of command to be excute(0-8): 5
(00)0                  Specifies an UNENCRYPTED password will follow
(01)7                  Specifies a HIDDEN password will follow
(02)LINE               The UNENCRYPTED <cleartext> user password
Please Input the code of command to be excute(0-2): 0
(00)LINE               The UNENCRYPTED <cleartext> user password
Please Input the code of command to be excute(0-0): 0
Please input a string:123456 ( Input password , here is only for example )
.....
(06)user-maxlinks     Limit the user's number of inbound links
(07)<cr>
Please Input the code of command to be excute(0-7): 7
Will you excute it? (Y/N):y

```

## 6.1.2.4 Examples of AAA Authentication Configuration

### 6.1.2.4.1 Examples of RADIUS Authentication

This section provides a sample configuration using RADIUS. The following example shows the process of how to configure the router to authenticate and authorize using RADIUS:

```
aaa authentication login radius-login radius local
aaa authentication ppp radius-ppp radius
aaa authorization network radius-network radius
line tty/vty
login authentication radius-login
interface serial 1/0
```

The command lines in this sample are defined as follows:

1. **aaa authentication login radius-login radius local** command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
2. **aaa authentication ppp radius-ppp radius** command configures the router as: to use **ppp** authentication using **chap** or **pap** if the user has not already logged in. If the **exec** facility has authenticated the user, PPP authentication is not performed.
3. **aaa authorization network radius-network radius** command queries **radius** for NETWORK service authorization.
4. **login authentication radius-login** command enables the **radius-login** method list for line 3.

#### 6.1.2.4.2 TACACS+ Authentication Example

The following example configures TACACS+ as the security protocol to be used for PPP authentication:

```
aaa authentication ppp test tacacs+ local
interface serial1\0
ppp authentication chap pap test
tacacs server 1.2.3.4
tacacs key testkey
```

The command lines in this sample TACACS+ authentication configuration are defined as follows:

**aaa authentication ppp test tacacs+** command defines a method list, “test,” to be used on serial interfaces running PPP. The keyword **tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

- **interface** command selects the port.
- **ppp authentication** command applies the test method list to this port.
- **tacacs-server** command identifies the TACACS+ server as having an IP address of 1.2.3.4
- **config-tacacs-server key** command defines the shared encryption key to be “testkey.”

The following example configures AAA authentication for PPP:

```
aaa authentication ppp default if-needed tacacs+ local
```

In this example, the keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP is not necessary and can be skipped. If authentication is needed, the keyword **tacacs+** means that authentication will be done through TACACS+ server. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the router.

The following example creates the same authentication algorithm for PAP but calls the method list “test-list” instead of “default”:

```
aaa authentication pap test-list if-needed tacacs+ local
```

```
interface serial1/0
ppp authentication pap test-list
```

In this example, since the list does not apply to any interfaces, the administrator must select interfaces to which this authentication scheme should apply by using the **config-interface** command. The administrator must then apply this method list to those interfaces by using the **ppp authentication** command.

## 6.2 Configure RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The "RADIUS Configuration Task List" section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set. The "RADIUS Authentication and Authorization Example" section at the end of this chapter offers two possible implementation scenarios.

“[RADIUS Configuration Task List](#)“ section introduce how to apply the commands of authentication, authorization and Accounting(AAA) to configure RADIUS. “[RADIUS Configuration Example](#)“ provide two examples at the last section of the chapter. Please refer to “[RADIUS Configuration Command](#)“ for complete description of RADIUS commands.

### 6.2.1 RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market. The router supports RADIUS under its AAA security paradigm. RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.

RADIUS is not suitable in the following network security situations:

RADIUS does not support the following protocols:

1. AppleTalk Remote Access (ARA) Protocol
2. NetBIOS Frame Control Protocol (NBFCP)
3. NetWare Asynchronous Services Interface (NASI)
4. X.25 PAD connections
5. Router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to

authenticate from one router to a non-Cisco router if the non-Cisco router requires RADIUS authentication.

6. Networks using a variety of services. RADIUS generally binds a user to one service model.

## 6.2.2 RADIUS Protocol Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

- The user is prompted for and enters a username and password.
- The username and encrypted password are sent over the network to the RADIUS server.
- The user receives one of the following responses from the RADIUS server.

**ACCEPT:**The user is authenticated.

**REJECT:**The user is not authenticated and is prompted to reenter the username and password, or access is denied.

**CHALLENGE:**A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or NETWORK authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

Services that the user can access, including Telnet, rlogin, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.

Connection parameters, including the host or client IP address, access list, and user timeouts.

## 6.2.3 RADIUS Configuration Steps

To configure RADIUS on the Router or access server, you must perform the following tasks:

Use *aaa authentication* global configuration command to define method lists for RADIUS authentication. For more information about using the *aaa authentication* command, refer to the "[Configuring Authentication](#)" chapter.

Use line and interface commands to enable the defined method lists to be used. For more information, refer to the "[Configuring Authentication](#)" chapter.

### 1. Configure Router to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider. A RADIUS server and a router use a shared secret key to encrypt passwords and exchange responses. Use the **radius server** command to specify the RADIUS server and use **radius key** to specify the shared key. use the following commands in global configuration directory:

| Step | Command                                                                                                              | Purpose                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>radius server</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ][ <b>acct-port</b> <i>portnumber</i> ] | Specify the IP address of the remote RADIUS server host and assign authentication and accounting destination port numbers. |
| 2    | <b>radius key</b> <i>string</i>                                                                                      | Specify the shared secret key used between the router and the RADIUS server.                                               |

Example: 1. To specify RADIUS server:

```
[DEFAULT@Router /config/]#radius
```

```
.....
```

```
(05)server                Specify a RADIUS server
(06)timeout              Time to wait for a RADIUS server to reply
(07)vsa                  Vendor specific attribute configuration
(08)test                 Radius test
Please Input the code of command to be excute(0-8): 5
```

```

(00)A.B.C.D                IP address of RADIUS server
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:192.168.0.1 (Input IP of the RADIUS server)
(00)acct-port              UDP port for RADIUS accounting server (default is 1646)
(01)auth-port              UDP port for RADIUS authentication server (default is 1645)
(02)<cr>
Please Input the code of command to be excute(0-2): 1
(00)<0-65536>              Port number
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:200
(00)acct-port              UDP port for RADIUS accounting server (default is 1646)
(01)<cr>
Please Input the code of command to be excute(0-1): 0
(00)<0-65536>              Port number
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:500
(00)<cr>
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y
2、 To specify the shared key of RADIUS server
[DEFAULT@Router /config/]#radius
(00)challenge-noecho      Data echoing to screen is disabled during Access-Challenge
(01)deadtime               Time to stop using a server that doesn't respond
(02)key                    Encryption key shared with the RADIUS servers
.....
Please Input the code of command to be excute(0-8): 2
(00)WORD                   Key string
Please Input the code of command to be excute(0-0): 0
Please input a string:123456 (Input key , here is only for example )
Will you excute it? (Y/N):y

```

To customize communication between the router and the RADIUS server, use the following optional radius global configuration commands:

| Step | Command                                 | Purpose                                                                                                                  |
|------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>radius retransmit</b> <i>retries</i> | Specify the number of times the router transmits each RADIUS request to the server before giving up (default is 2).      |
| 2    | <b>radius timeout</b> <i>seconds</i>    | Specify the number of seconds a router waits for a reply to a RADIUS request before retransmitting the request.          |
| 3    | <b>radius deadtime</b> <i>minutes</i>   | Specify the number of minutes that marked a RADIUS server as “dead”, which is not responding to authentication requests. |

**Example:**

```

[DEFAULT@Router /config/]#radius
.....
(04)retransmit             Search iterations of the RADIUS server list
(05)server                 Specify a RADIUS server
.....

```

```

Please Input the code of command to be excute(0-8): 4
(00)<0-100>                               Number of times to retransmit (default 2)
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:5 (Input retris ,here is only for example)
Will you excute it? (Y/N):y
[DEFAULT@Router /config/]#radius
.....
(06)timeout                               Time to wait for a RADIUS server to reply
(07)vsa                                    Vendor specific attribute configuration
(08)test                                   Radius test
Please Input the code of command to be excute(0-8): 6
(00)<1-1000>                               Wait timeout in seconds
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:30 (Input the time value of timeout ,here is only for
example)
Will you excute it? (Y/N):y
[DEFAULT@Router /config/]#radius
(00)challenge-noecho                      Data echoing to screen is disabled during Access-Challenge
(01)deadtime                              Time to stop using a server that doesn't respond
.....
Please Input the code of command to be excute(0-8): 1
(00)<0-1440>                               Time in minutes
Please Input the code of command to be excute(0-0): 0
Please input a digital number:Please input a string:60 (Input the time value of deadtime ,here is only for
example)
Will you excute it? (Y/N):y

```

### 6.2.3.2 Configure Router To Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (Attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. For more information about vendor-IDs and VSAs, refer to RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)." To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

| Command                          | Purpose                                                                                            |
|----------------------------------|----------------------------------------------------------------------------------------------------|
| radius vsa send [authentication] | Enable the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26. |

Example:

```

[DEFAULT@Router /config/]#radius
.....
(07)vsa                                    Vendor specific attribute configuration
(08)test                                   Radius test
Please Input the code of command to be excute(0-8): 7
(00)send                                   Send vendor-specific attributes in requests
Please Input the code of command to be excute(0-0): 0
(00)authentication                        Send in access requests
(01)<cr>

```

```
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y
```

### 6.2.3.3 Configure Radius Autentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you need to define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you need to enter the **aaa authentication** command, specifying RADIUS as the authentication method. For more information, refer to the "Configuring Authentication" chapter.

### 6.2.3.4 Configure Radius Authorization

AAA authorization lets you set parameters that restrict a user's network access. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you need to issue the **aaa authorization** command, specifying RADIUS as the authorization method. For more information, refer to the "Configuring Authorization" chapter.

### 6.2.3.5 Configure Radius Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you need to issue **aaa accounting** command, specifying RADIUS as the accounting method. For more information, refer to the "Configuring Accounting" chapter.

## 6.2.4 RADIUS Configuration Examples

Radius configuration examples in this section include the following:

- RADIUS authentication examples
- RADIUS examples in AAA application

### 6.2.4.1 Radius Authentication and Authorization Examples

The following example shows how to configure the router to authenticate and authorize using RADIUS:

```
aaa authentication login use-radius radius local
aaa authentication ppp use-radius if-needed radius
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

**aaa authentication login use-radius radius local** command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication.

**aaa authentication ppp user-radius if-needed radius** command configures the router to use RADIUS authentication for lines using Point-to-Point Protocol (PPP) with CHAP or PAP if the user has not already been authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the **if-needed** authentication method.

### 6.2.4.2 Radius Examples In AAA Application

The following example is a general configuration using RADIUS with the AAA command set:

```
radius server 1.2.3.4
radius key myRaDiUSpassWoRd
username root password AlongPassword
aaa authentication ppp dialins radius local
```

```

aaa authentication login admins local
line 1 16
login authentication admins
interface async0/0
encap ppp
ppp authentication pap dialins

```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

**radius-server** command defines the IP address of the RADIUS server.

**set-priority-group** command defines the shared secret key of network access server and RADIUS server host.

**aaa authentication ppp dialins radius local** command defines the authentication method list "dialins," which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used.

**ppp authentication pap dialins** command applies the "dialins" method list to the lines specified.

The aaa authorization network radius local command is used to assign an address and other network parameters to the RADIUS user.

**aaa authentication login admins local** command defines another method list, "admins," for login authentication.

**login authentication admins** command applies the "admins" method list for login authentication.

## 6.3 Configure TACACS+ Directory

### 6.3.1 TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. The security of communication can be ensured for the network access server and TACACS+ service program exchange the encrypted messages.

You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.

**Authentication---**Supported multiple authentication methods (ASCII, PAP, CHAP). The authentication facility provides the ability to conduct an arbitrary dialog with the user (for example, after a login and password are provided, to challenge a user with a number of questions, like home address, service type, and ID card number). In addition, the TACACS+ authentication service supports sending messages to user screens. For example, a message could notify users that their passwords must be changed because of the company's password aging policy.

**Authorization---**Provides fine-grained control over user capabilities for the duration of the user's session, including but not limited to setting autocommands, access control, session duration. You can also enforce restrictions on what commands a user may executed.

**Accounting---**Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

### 6.3.2 TACACS+ Protocol Operation

#### 6.3.2.1 ASCII Mode Authentication

When a user attempts a simple ASCII login by authenticating to a network access server using TACACS+, the following process typically occurs:

When the connection is established, the network access server will contact the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username and the network access server then contacts the TACACS+ daemon to obtain a password prompt. The network access server displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ service program.

**Note: TACACS+ allows an arbitrary conversation to be held between the daemon and the user until the daemon receives enough information to authenticate the user. This is usually done by prompting for a username and password combination, but may include other items, such as mother's maiden name, all under the control of the TACACS+ service program.**

The network access server will eventually receive one of the following responses from the TACACS+ server:

|                 |                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACCEPT</b>   | The user is authenticated and service may begin. If the network access server is configured to require authorization, authorization will begin at this time.                                                                                                                                                   |
| <b>REJECT</b>   | The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending on the processing type of TACACS+ server.                                                                                                                                |
| <b>ERROR</b>    | An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the network access server. If an ERROR response is received, the network access server will typically try to use an alternative method for authenticating the user. |
| <b>CONTINUE</b> | The user is prompted for additional authentication information.                                                                                                                                                                                                                                                |

#### 6.3.2.2 PAP & CHAP Mode Authentication

A PAP login is similar to an ASCII login, except that the username and password arrive at the network access server in a PAP protocol packet instead of being typed in by the user, so the user is not prompted. PPP CHAP logins are also similar in principle. Following authentication, the user will also be required to undergo an additional authorization phase, if authorization has been enabled on the network access server. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

If TACACS+ authorization is required, the TACACS+ service program is again contacted and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response will contain data in the form of attributes that are used to direct the EXEC or NETWORK session for that user, determining services that the user can access.

### 6.3.3 TACACS+ Configuration Process

To configure your router to support TACACS+, you must perform the following tasks:

- ◆ Use the **tacacs-server** command to specify the IP address of one or more TACACS+ server. Use the **config-tacacs key** command to specify an encryption key that will be used to encrypt all exchanges between the network access server and the TACACS+ server. This same key must also be configured on the TACACS+ service program.
- ◆ Use the **aaa authentication global configuration** command to define method lists that use TACACS+ for authentication. For more information about using the **aaa authentication** command, refer to the "[Configuring Authentication](#)" chapter.
- ◆ Use **line and interface** commands to apply the defined method lists to various interfaces. For more information, refer to the "[Configuring Authentication](#)" chapter.

#### 6.3.3.1 Specify A TACACS+ Server

**tacacs server** command enables you to specify the names of the IP host or hosts maintaining a TACACS+ server. Because the TACACS+ software searches for the hosts in the order specified, this feature can be useful for setting up a list of

preferred servers. To specify a TACACS+ host, use the following command in global configuration mode:

| Command                                                                                                                                    | Purpose                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| tacacs server <i>ip-address</i> [single-connection multi-connection] [port <i>integer</i> ] [timeout <i>integer</i> ] [key <i>string</i> ] | Specify the IP address and correlative attribute of TACACS+ server. |

```
[DEFAULT@Router /config/]#tacacs
```

```
Key Word:
```

```
U(undo) D(default) Q(quit)
```

```
(00)server Config TACACS+ server
```

```
(01)key Default TACACS+ key
```

```
(02)timeout Config session timeout value
```

```
Please Input the code of command to be excute(0-2): 0
```

```
Key Word:
```

```
Q(quit)
```

```
(00)A.B.C.D TACACS+ host IP address
```

```
Please Input the code of command to be excute(0-0): 0
```

```
Please input a IP Address:10.0.0.1 (Input TACACS+ host IP address)
```

```
Key Word:
```

```
Q(quit)
```

```
.....
```

```
(03)single-connect Through single TCP connection
```

```
(04)multi-connect Through single TCP connection
```

```
(05)<cr>
```

```
Please Input the code of command to be excute(0-5): 3
```

```
Key Word:
```

```
Q(quit)
```

```
(00)key Config TACACS+ key
```

```
(01)port Config TACACS+ port number
```

```
(02)timeout Wait timeout in seconds
```

```
(03)<cr>
```

```
Please Input the code of command to be excute(0-3): 1
```

```
Key Word:
```

```
Q(quit)
```

```
(00)<1-65535> Port number
```

```
Please Input the code of command to be excute(0-0): 0
```

```
Please input a digital number:100 (Input Port number)
```

```
Key Word:
```

```
Q(quit)
```

```
(00)key Config TACACS+ key
```

```
(01)timeout Wait timeout in seconds
```

```
(02)<cr>
```

```
Please Input the code of command to be excute(0-2): 1
```

```
Key Word:
```

```
Q(quit)
```

```
(00)<1-600> Seconds
```

```
Please Input the code of command to be excute(0-0): 0
```

```
Please input a digital number:300 (Input timeout value)
```

```
Key Word:
```

```
Q(quit)
```

```
(00)key Config TACACS+ key
```

```
(01)<cr>
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00)WORD                               Key string
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom (Input key string)
Key Word:
Q(quit)
(00)<cr>
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y
```

Using the **tacacs-server** command, you can also configure the following options:

- Use the **single-connection** keyword to specify single-connection. This is more efficient because it allows the server to handle a higher number of TACACS operations. The **multi-connection** keyword means multiple TCP connection.
- Use the port integer argument to specify the TCP port number to be used when making connections to the TACACS+ server. The default port number is 49.
- Use the **timeout** integer argument to specify the period of time (in seconds) the router will wait for a response from the server.
- Use the key string argument to specify an encryption key for encrypting and decrypting all traffic.

**Note: Specifying the encryption key with the tacacs-server command overrides the default key set by the global configuration config-tacacs server key command; Specifying the timeout value with the tacacs-server command overrides the global timeout value set with the config-tacacs server timeout command. You can use this command to enhance security on your network by uniquely configuring individual TACACS+ connections.**

### 6.3.3.2 Set TACACS+ Encryption Key

To set the TACACS+ authentication key and encryption key, use the following command in global configuration mode:

| Command                            | Purpose                                                          |
|------------------------------------|------------------------------------------------------------------|
| <b>tacacs key</b> <i>keystring</i> | Set the encryption key to match that used on the TACACS+ server. |

```
[DEFAULT@Router /config/]#tacacs
Key Word:
U(undo) D(default)          Q(quit)
(00)server                   Config TACACS+ server
(01)key                       Default TACACS+ key
(02)timeout                  Config session timeout value
Please Input the code of command to be excute(0-2): 1
Key Word:
Q(quit)
(00)WORD                     TACACS+ key (max 31 character)
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom (Input TACACS+ key string)
Will you excute it? (Y/N):y
```

Note: You must configure the same key on the TACACS+ server for encryption to be successful.

### 6.3.3.3 Specify TACACS+ Authentication

After you have identified the TACACS+ daemon and defined an associated TACACS+ encryption key, you need to define

method lists for TACACS+ authentication. Because TACACS+ authentication is operated via AAA, you need to set **aaa authentication** command, specifying TACACS+ as the authentication method. For more information, refer to the "[Configuring Authentication](#)" chapter.

#### 6.3.3.4 Specify TACACS+ Authorization

AAA authorization enables you to set parameters that restrict a user's network access. Authorization via TACACS+ may be applied to commands, network connections, and EXEC sessions. Because TACACS+ authorization is facilitated through AAA, you need to issue the **config-aaa authorization** command, specifying TACACS+ as the authorization method. For more information, refer to the "Configuring Authorization" chapter.

#### 6.3.3.5 Specify TACACS+ Accounting

AAA accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because TACACS+ accounting is facilitated through AAA, you need to issue the **aaa accounting** command, specifying TACACS+ as the accounting method. For more information, refer to the "Configuring Accounting" chapter.

### 6.3.4 TACACS+ Configuration Examples

This section describes the following TACACS+ configuration examples:

#### [TACACS+ Authentication Examples](#)

##### 6.3.4.1 TACACS+ Authentication Examples

The following example configures TACACS+ as the security protocol to be used for PPP authentication:

```
aaa authentication ppp test tacacs+ local
tacacs server 1.2.3.4
tacacs key testkey
interface serial 1/1
ppp authentication chap pap test
```

In this example:

**aaa authentication** command defines a method list, "test," to be used on serial interfaces running PPP. The keyword **tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

**Tacacs server** command identifies the TACACS+ server as having an IP address of 10.1.2.3. The **config-tacacs key** command defines the shared encryption key to be "testkey."

**interface** command selects the port, and the **ppp authentication** command applies the test method list to this port.

The following example configures TACACS+ as the security protocol to be used for PPP authentication but instead of the method list "test," the method list, "default," is used.

```
aaa authentication ppp default if-needed tacacs+ local
tacacs-server host 1.2.3.4
tacacs-server key goaway
interface serial 1/1
ppp (default) authentication
```

In this example:

**aaa authentication** command defines a method list, "default," to be used on serial interfaces running PPP. The **if-needed** keyword means that if the user has already authenticated, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **tacacs+** means that authentication will be done through TACACS+. If TACACS+

returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

**Tacacs server** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **config-tacacs key** command defines the shared encryption key to be "goaway."

**interface** command selects the port, and the **ppp authentication** command applies the default PPP method list to this port.

#### 6.3.4.2 TACACS+ Authorization Example

```
aaa authentication ppp default if-needed tacacs+ local
aaa authorization network default tacacs+
tacacs server 10.1.2.3
tacacs key goaway
interface serial 1/1
ppp (default) authentication
ppp (default) authorization
```

In this example:

**aaa authentication** command defines a method list, "default," to be used on serial interfaces running PPP. The **if-needed** keyword means that if the user has already authenticated, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

**aaa authorization** command configures network authorization via TACACS+.

**Tacacs server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. **tacacs server key** command defines the shared encryption key to be "goaway."

**interface** command selects the line, and the **ppp authentication** command and the **ppp authorization** applies the default authentication or authorization method list to this port.

#### 6.3.4.3 TACACS+ Accounting Example

```
aaa authentication ppp default if-needed tacacs+ local
aaa accounting network default stop-only tacacs+
tacacs server 10.1.2.3
tacacs key goaway
interface serial 1/1
ppp (default) authentication
ppp (default) accounting
```

In this example:

**aaa authentication** command defines a method list, "default," to be used on serial interfaces running PPP. **if-needed** keyword means that if the user has already authenticated, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

**aaa accounting** command configures network accounting via TACACS+. In this example, accounting records describing the session that just terminated will be sent to the TACACS+ server whenever a network connection terminates.

**Tacacs server** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. **tacacs key** command defines the shared encryption key to be "goaway."

**interface** command selects the port, and the **ppp authentication** command applies the default method list to this port; **ppp-accounting** command applies the default method list to this port.

## 6.4 Configure IPsec

### 6.4.1 About Configure IPsec

This chapter describes how to configure IPsec, which is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices, such as D-Link routers.

IPsec provides the following network security services. These services are optional. In general, local security policy will dictate the use of one or more of these services:

- **Data Confidentiality**—The IPsec sender can encrypt packets before transmitting them across a network.
- **Data Integrity**—The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- **Data Origin Authentication**—The IPsec receiver can authenticate the source of the IPsec packets sent. This service is dependent upon the data integrity service.
- **Anti-Replay**—The IPsec receiver can detect and reject replayed packets.

With IPsec, data can be transmitted across a public network without fear of observation, modification, or spoofing. For a complete description of the IPsec commands used in this chapter, refer to the "[IPsec Configuration Command](#)" chapter.

### 6.4.2 IPsec Overview

IPsec provides network data encryption at the IP packet level, offering a robust security solution that is standards-based. IPsec provides data authentication and anti-replay services in addition to data confidentiality services.

#### 6.4.2.1 Supported Standards

The Router implements the following standards with this feature:

- **IPsec—IP Security Protocol.** IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
- **Internet Key Exchange (IKE)**—A hybrid protocol that implements Oakley and SKEME key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of the IPsec peers, negotiates IPsec security associations, and establishes IPsec keys. For more information on IKE, see the chapter "Configuring Internet Key Exchange Security Protocol."

The component technologies implemented for IPsec include:

- **DES**—The Data Encryption Standard (DES) is used to encrypt packet data. D-Link router implements the mandatory 56-bit DES-CBC with IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption.
- **3DES**—Triple DES (3DES) is a symmetric encrypting algorithm that encrypts the packet data. D-Link router adopted DES-CBC with 168-bit 3DES is more security than DES.
- **MD5 (HMAC variant)**—MD5 (Message Digest 5) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- **SHA (HMAC variant)**—SHA (Secure Hash Algorithm) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

Router IPsec supports the following additional standards:

- **AH**—Authentication Header. A security protocol which provides data authentication of data integrity, data

origin authentication and optional anti-replay services. AH is use to protect an upper level protocol (transmitting mode) and a full IP datagram (channel mode). AH is defined in RFC2402. It can be used independently or gathered with ESP.

- ESP—Encapsulating Security Payload. A security protocol which provides data privacy services include data confidentiality, data origin authentication, anti-replay and data integrity services. ESP is use to protect an upper level protocol (transmitting mode) and a full IP datagram (channel mode). AH is defined in RFC2406.

#### 6.4.2.2 Terms

Security Parameter Index (SPI)

Security Association

Transform

anti-replay

Perfect Forward Secrecy (PFS)

Data Flow

Data Authentication

#### 6.4.2.3 Restrictions

At this time, IPsec can be applied to unicast IP datagrams only. Because the IPsec Working Group has not yet addressed the issue of group key distribution, IPsec does not currently work with multicasts or broadcast IP datagrams. If you use Network Address Translation (NAT), you should configure static NAT translations so that IPsec will work properly. In general, NAT translation should occur before the router performs IPsec encapsulation; in other words, IPsec should be working with global addresses.

#### 6.4.3 Overview of How IPsec Works

IPsec provides secure tunnels between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters which should be used to protect these sensitive packets, by specifying characteristics of these tunnels. Then, when the IPsec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these tunnels are sets of security associations that are established between two IPsec peers. The security associations define which protocols and algorithms should be applied to sensitive packets, and also specify the keying material to be used by the two peers. Security associations are unidirectional and are established per security protocol (AH or ESP).

With IPsec you define what traffic should be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces by way of crypto map sets. Therefore, traffic may be selected based on source and destination address, and optionally Layer 4 protocol, and port. (The access lists used for IPsec are used only to determine which traffic should be protected by IPsec, not which traffic should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.) A crypto map set can contain multiple entries, each with a different access list.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If no security association exists that IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec security associations.

If the crypto map entry is tagged as **ipsec-manual**, IPsec is triggered. If no security association exists that IPsec can use to protect this traffic to the peer, the traffic is dropped. In this case, the security associations are installed via the configuration, without the intervention of IKE. If the security associations did not exist, IPsec did not have all of the

necessary pieces configured.

Once established, the set of security associations (outbound, to the peer) is then applied to the triggering packet as well as to subsequent applicable packets as those packets exit the router. "Applicable" packets are packets that match the same access list criteria that the original packet matched.

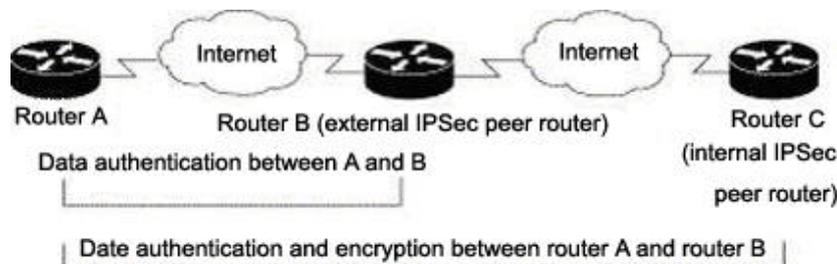
If IKE is used to establish the security associations, the security associations will have lifetimes so that they will periodically expire and require renegotiation. (This provides an additional level of security.)

Multiple IPSec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of security associations. For example, some data streams might be just authenticated while other data streams must both be encrypted and authenticated. Access lists associated with IPSec crypto map entries also represent which traffic the router requires to be protected by IPSec. Inbound traffic is processed against the crypto map entries—if an unprotected packet matches a permit entry in a particular access list associated with an IPSec crypto map entry, that packet is dropped because it was not sent as an IPSec-protected packet. Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IPSec protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

#### 6.4.3.1 Nesting Of IPSec

You can nest IPSec traffic to a series of IPSec peers. For example, in order for traffic to traverse multiple firewalls (and these firewalls have a policy of not letting through traffic that they themselves have not authenticated), the router needs to establish IPSec tunnels with each firewall in turn.

In the example shown, Router A encapsulates the traffic destined for Router C in IPSec (Router C is the IPSec peer). However, before Router A can send this traffic, it must first reencapsulate this traffic in IPSec in order to send it to Router B.



Nesting Example of IPSec Peers

It is possible for the traffic between the "outer" peers to have one kind of protection (such as data authentication) and for traffic between the "inner" peers to have different protection (such as both data authentication and encryption).

#### 6.4.4 IPSec Configuration Steps

After you have completed IKE configuration, configure IPSec by completing the following tasks at each participating IPSec peer:

[Ensuring That Access Lists Are Compatible with IPSec](#)

[Creating Crypto Access Lists](#)

[Defining Transform Sets](#)

[Creating Crypto Map Entries](#)

[Applying Crypto Map Sets to Interfaces](#)

### 6.4.4.1 Ensuring That Access Lists Are Compatible With IPSec

IKE uses UDP port 500. The IPSec ESP and AH protocols use protocol numbers 50 and 51. Ensure that your access lists are configured so that protocol 50, 51, and UDP port 500 traffic is not blocked at interfaces used by IPSec.

### 6.4.4.2 Creat Crypto Access Lists

Crypto access lists are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. (These access lists are not the same as regular access lists, which determine what traffic to forward or block at an interface.)

Crypto access lists associated with IPSec crypto map entries have four primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new security associations (specified by a single **permit** entry) when initiating negotiations for IPSec security associations.
- Process inbound traffic in order to filter out and discard traffic that should have been protected by IPSec.
- Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the IPSec peer.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries which specify different IPSec policies.

Later, you will associate the crypto access lists to particular interfaces when you configure and apply crypto map sets to the interfaces. To create crypto access lists, use the following command in global configuration mode:

| Command                                                                                                                                                 | Purpose                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <b>ip access-list extended</b> name 然后使用 <b>permit</b> 和 <b>deny</b> 命令设置访问规则<br><b>permit</b> protocol source source-mask destination destination-mask | Specifies which IP packets will be encrypting protected. |

```
[DEFAULT@Router /config/]#ip
  Key Word:
  U(undo) D(default)          Q(quit)
  (00)access-list              Named access-list
  (01)as-path                  BGP as-path access list definition
  .....
  Please Input the code of command to be excute(0-20): 0
  Key Word:
  Q(quit)
  (00)extended                 Extended Access List
  (01)standard                 Standard Access List
  Please Input the code of command to be excute(0-1): 0
  Key Word:
  Q(quit)
  (00)WORD                     Extended Access-list name
  Please Input the code of command to be excute(0-0): 0
  Please input a string:bdcom (Input Access-list name)
  Will you excute it? (Y/N):y
  Key Word:
  Q(quit)
  .....
  (11)permit                   Specify packets to forward
  (13)router                   routing protocol configuration
  .....
  Please Input the code of command to be excute(0-14): 11
```

```

Key Word:
U(undo) D(default)      Q(quit)
.....
(03)ip                  Internet Protocol
(04)ospf                OSPF routing protocol
(05)tcp                 Transmission Control Protocol
(06)udp                 User Datagram Protocol
Please Input the code of command to be excute(0-6): 3
Key Word:
Q(quit)
(00)A.B.C.D            Address to match
(01)any                Any source host
Please Input the code of command to be excute(0-1): 0
Please input a IP Address:192.168.1.0 255.255.255.0 ( Input source ip address )
Key Word:
Q(quit)
(00)A.B.C.D            Address to match
(01)any                Any destination host
Please Input the code of command to be excute(0-1): 0
Please input a IP Address:192.168.2.0 255.255.255.0 ( Input dest ip address )
Key Word:
Q(quit)
.....
(03)precedence         Match packets with given precedence value
(04)<cr>
Please Input the code of command to be excute(0-4): 4
Will you excute it? (Y/N):y

```

### Crypto Access List Tips

Using the **permit** keyword causes all IP traffic that matches the specified conditions to be protected by crypto, using the policy described by the corresponding crypto map entry. Using the **deny** keyword prevents traffic from being protected by crypto in the context of that particular crypto map entry. (In other words, it does not allow the policy as specified in this crypto map entry to be applied to this traffic.) If this traffic is denied in all of the crypto map entries for that interface, then the traffic is not protected by crypto.

The crypto access list you define will be applied to an interface after you define the corresponding crypto map entry and apply the crypto map set to the interface. Different access lists must be used in different entries of the same crypto map set. (These two tasks are described in following sections.) However, both inbound and outbound traffic will be evaluated against the same "outbound" IPSec access list. Therefore, the access list's criteria is applied in the forward direction to traffic exiting your router, and the reverse direction to traffic entering your router.

If you configure multiple statements for a given crypto access list which is used for IPSec, only the first permit statement is useful.

### Using the any Keyword in Crypto Access Lists

When you create crypto access lists, using the **any** keyword could cause problems. D-Link discourages the use of the **any** keyword to specify source or destination addresses.

The **any** keyword in a **permit** statement is discouraged when you have multicast traffic flowing through the IPSec interface; the **any** keyword can cause multicast traffic to fail. The **permit any any** statement is strongly discouraged, as this will cause all outbound traffic to be protected (and all protected traffic sent to the peer specified in the corresponding crypto map entry) and will require protection for all inbound traffic.

### 6.4.4.3 Define Transform Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry.

During IPsec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of both peers' IPsec security associations.

With manually established security associations, there is no negotiation with the peer, so both sides must specify the same transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command.

To define a transform set, use the following commands starting in global configuration mode:

| Step | Command                                                        | Purpose                                                                                                                                                                                                                                                             |
|------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>crypto ipsec transform-set</b><br><i>transform-set-name</i> | Defines a transform set and perform this command into the crypto transform configuration mode.                                                                                                                                                                      |
| 2    | <b>transform-type</b> transform1<br>[transform2[transform3]]   | Configure transform type.                                                                                                                                                                                                                                           |
| 3    | <b>mode</b> [tunnel   transport]                               | (Optional) Changes the mode associated with the transform set. The mode setting is only applicable to traffic whose source and destination addresses are the IPsec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) |
| 4    | <b>exit</b>                                                    | Exits the crypto transform configuration mode.                                                                                                                                                                                                                      |

```
[DEFAULT@Router /config/]#crypto
```

```
Key Word:
```

```
U(undo) D(default) Q(quit)
```

```
(00)dynamic-map Specify a dynamic crypto map template
```

```
(01)ipsec Configure IPSEC policy
```

```
(02)isakmp Configure ISAKMP policy
```

```
(03)map Enter a crypto map
```

```
Please Input the code of command to be excute(0-3): 1
```

```
Key Word:
```

```
Q(quit)
```

```
(00)transform-set Define transform and settings
```

```
(01)secure Only allow secure ip packets
```

```
Please Input the code of command to be excute(0-1): 0
```

```
Key Word:
```

```
Q(quit)
```

```
(00)WORD Transform set name
```

```
Please Input the code of command to be excute(0-0): 0
```

```
Please input a string:bdcom (Input Transform set name, here is only for example)
```

```

Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(18)transform-type          transform type
(19)where                   display all outgoing telnet connection
Please Input the code of command to be excute(0-19): 18
Key Word:
U(undo) D(default)        Q(quit)
.....
(04)esp-md5-hmac           ESP transform using HMAC-MD5 auth
(05)esp-null ESP           transform w/o cipher
(06)esp-sha-hmac           ESP transform using HMAC-SHA auth
Please Input the code of command to be excute(0-6): 4
Key Word:
Q(quit)
.....
(04)esp-null               ESP transform w/o cipher
(05)<CR>
Please Input the code of command to be excute(0-5): 5
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(10)interface              interface configuration
(11)mode                   encapsulation mode (transport/tunnel)
.....
Please Input the code of command to be excute(0-19): 11
Key Word:
U(undo) D(default)        Q(quit)
(00)transport              transport (payload encapsulation) mode
(01)tunnel                 tunnel (datagram encapsulation) mode
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(05)english                help message in English
(06)exit                   exit / quit
.....
Please Input the code of command to be excute(0-19): 6
Will you excute it? (Y/N):y

```

Following table shows allowed transform combinations.

| Select transform for transform set: Allowed Transform Combinations |                 |                          |                  |                             |                  |
|--------------------------------------------------------------------|-----------------|--------------------------|------------------|-----------------------------|------------------|
| AH Transform                                                       |                 | ESP Encryption Transform |                  | ESP Authentication Transorm |                  |
| Transform                                                          | Description     | Transform                | Description      | Transform                   | Description      |
| ah-md5-hmac                                                        | AH with the MD5 | esp-des                  | ESP with the DES | esp-md5-hmac                | ESP with the MD5 |

|             |                                                               |          |                                           |              |                                                                |
|-------------|---------------------------------------------------------------|----------|-------------------------------------------|--------------|----------------------------------------------------------------|
|             | (HMAC variant)<br>authentication algorithm                    |          | encryption algorithm                      |              | (HMAC variant)<br>authentication algorithm                     |
| ah-sha-hmac | AH with the SHA<br>(HMAC variant)<br>authentication algorithm | esp-3des | ESP with the 3DES<br>encryption algorithm | esp-sha-hmac | ESP with the SHA<br>(HMAC variant)<br>authentication algorithm |

#### 6.4.4.4 Creat Crypto Map Entries

##### About Crypto Map Entries

Crypto map entries created for IPSec including:

- Which traffic should be protected by IPSec (per a crypto access list)
- The granularity of the flow to be protected by a set of security associations
- The local address to be used for the IPSec traffic
- The peer address to be used for the IPSec traffic
- What IPSec security should be applied to this traffic (selecting from a list of one or more transform sets)
- Whether security associations are manually established or are established via IKE
- Other parameters that might be necessary to define an IPSec security association

Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set. Later, you will apply these crypto map sets to interfaces; then, all IP traffic passing through the interface is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, a security association is negotiated with the remote peer according to the parameters included in the crypto map entry; otherwise, if the crypto map entry specifies the use of manual security associations, a security association should have already been established via configuration. If the local router initiates the negotiation, it will use the policy specified in the static crypto map entries to create the offer to be sent to the specified IPSec peer. If the IPSec peer initiates the negotiation, the local router will check the policy from the static crypto map entries, as well as any referenced dynamic crypto map entries to decide whether to accept or reject the peer's request .

For IPSec to succeed between two IPSec peers, both peers' crypto map entries must contain compatible configuration statements.

When two peers try to establish a security association, they must each have at least one crypto map entry that is compatible with one of the other peer's crypto map entries. For two crypto map entries to be compatible, they must at least meet the following criteria:

- The crypto map entries must contain compatible crypto access lists.
- The crypto map entries must each identify the other peer.
- The crypto map entries must have at least one transform set in common.

#### How Many Crypto Maps Should You Create

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPSec/IKE and IPSec/manual entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

If you create more than one crypto map entry for a given interface, use the seq-num of each map entry to rank the map entries: the lower the seq-num, the higher the priority. At the interface that has the crypto map set, traffic is evaluated against higher priority map entries first. You must create multiple crypto map entries for a given interface if any of the following conditions exist:

1. If different data flows are to be handled by separate IPSec peers.
2. If you want to apply different IPSec security to different types of traffic (to the same or separate IPSec peers); for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case the different types of traffic should have been

- defined in two separate access lists, and you must create a separate crypto map entry for each crypto access list.
- If you are not using IKE to establish a particular set of security associations, and want to specify multiple access list entries, you must create separate access lists (one per permit entry) and specify a separate crypto map entry for each access list.

### Creating Crypto Map Entries Manually

The use of manual security associations is a result of a prior arrangement between the users of the local router and the IPSec peer. The two parties may wish to begin with manual security associations, and then move to using security associations established via IKE, or the remote party's system may not support IKE. If IKE is not used for establishing the security associations, there is no negotiation of security associations, so the configuration information in both systems must be the same in order for traffic to be processed successfully by IPSec.

The local router can simultaneously support manual and IKE-established security associations.

To create crypto map entries to establish manual security associations, use the following commands starting in global configuration mode:

| Step | Command                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>crypto map</b> <i>map-name seq-num</i><br><b>ipsec-manual</b>                                                                                                                                                                                                                                     | Specifies the crypto map entry to create (or modify). Perform this command into the crypto map configuration mode.                                                                                                                                                                                                                                                                                                                                   |
| 2    | <b>match address</b> access-list-name                                                                                                                                                                                                                                                                | Configure an IPSec access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry.                                                                                                                                                                                                                                          |
| 3    | <b>set peer</b> ip-address                                                                                                                                                                                                                                                                           | Specifies the address of IPSec peer. This is the address to which IPSec protected traffic should be forwarded.                                                                                                                                                                                                                                                                                                                                       |
| 4    | <b>set transform-set</b><br><i>transform-set-name</i>                                                                                                                                                                                                                                                | Specifies the transform set. (Only one transform set can be specified for <b>ipsec-manual</b> crypto map entries. For <b>ipsec-isakmp</b> crypto map entries, no more than six transform sets can be specified.)                                                                                                                                                                                                                                     |
| 5    | <b>set security-association inbound</b><br><b>ah</b> <i>spi hex-key-data</i> 和 <b>set</b><br><b>security-association outbound</b><br><b>ah</b> <i>spi hex-key-data</i>                                                                                                                               | Sets the AH Security Parameter Indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the AH protocol. This command manually specifies the AH security association to be used with protected traffic.                                                                                                                                                                                    |
| 6    | <b>set security-association inbound</b><br><b>esp</b> <i>spi [cipher</i><br><i>hex-key-data]</i> [ <b>authenticator</b><br><i>hex-key-data</i> ] 和 <b>set</b><br><b>security-association outbound</b><br><b>esp</b> <i>spi [cipher hex-key-data]</i><br>[ <b>authenticator</b> <i>hex-key-data</i> ] | Sets the ESP Security Parameter Indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the ESP protocol. Specifies the cipher keys if the transform set includes an ESP cipher algorithm. Specifies the authenticator keys if the transform set includes an ESP authenticator algorithm. This command manually specifies the ESP security association to be used with protected traffic. |
| 7    | <b>exit</b>                                                                                                                                                                                                                                                                                          | Exits crypto-map configuration mode and return to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                         |

```
[DEFAULT@Router /config/]#crypto
```

Key Word:

U(undo) D(default)

Q(quit)

(00)dynamic-map

Specify a dynamic crypto map template

(01)ipsec

Configure IPSEC policy

(02)isakmp

Configure ISAKMP policy

```

(03)map                                Enter a crypto map
Please Input the code of command to be excute(0-3): 3
Key Word:
Q(quit)
(00)WORD                                Crypto map name
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom (Input crypto map name)
Key Word:
Q(quit)
(00)<0-65535>                            Sequence to insert into crypto map entry
(01)local-address                        Interface to use for local address for this crypto map
Please Input the code of command to be excute(0-1): 0
Please input a digital number:100 (Input Sequence Value)
Key Word:
Q(quit)
(00)ipsec-isakmp                        IPSEC w/ISAKMP
(01)ipsec-manual                        IPSEC w/manual keying
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(10)interface                            interface configuration
(11)match                                Match values
.....
Please Input the code of command to be excute(0-19): 11
Key Word:
U(undo) D(default) Q(quit)
(00)address                              Match address of packets to encrypt.
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)WORD                                Access-list name
Please Input the code of command to be excute(0-0): 0
Please input a string:bdcom (Input Access-list name)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(16)set                                  Set values for encryption/decryption
(17)show                                  show configuration and status
.....
Please Input the code of command to be excute(0-19): 16
Key Word:
U(undo) D(default) Q(quit)
(00)peer                                  Allowed Encryption/Decryption peer.
(01)security-association                  Security association parameters
(02)transform-set                        Specify list of transform sets
Please Input the code of command to be excute(0-2): 0

```

```

Key Word:
Q(quit)
(00)A.B.C.D IP          address of peer
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:10.0.0.1 (Input peer ip Address)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(16)set                Set values for encryption/decryption
(17)show              show configuration and status
.....
Please Input the code of command to be excute(0-19): 16
Key Word:
U(undo) D(default)    Q(quit)
(00)peer              Allowed Encryption/Decryption peer.
(01)security-association Security association parameters
(02)transform-set     Specify list of transform sets
Please Input the code of command to be excute(0-2): 1
Key Word:
Q(quit)
(00)inbound           Inbound manual security association
(01)outbound          Outbound manual security association
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00)ah                AH key
(01)esp               ESP key
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00)<256-4294967295>  SPI for security association
Please Input the code of command to be excute(0-0): 0
Please input a digital number:10000 (Input SPI Value)
Key Word:
Q(quit)
(00)WORD              security association key value (hex w/o leading 0x)
Please Input the code of command to be excute(0-0): 0
Please input a string:123456 (Input association key value)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(16)set                Set values for encryption/decryption
(17)show              show configuration and status
.....
Please Input the code of command to be excute(0-19): 16
Key Word:
U(undo) D(default)    Q(quit)

```

```

(00)peer                Allowed Encryption/Decryption peer.
(01)security-association Security association parameters
(02)transform-set       Specify list of transform sets
Please Input the code of command to be excute(0-2): 1
Key Word:
Q(quit)
(00)inbound            Inbound manual security association
(01)outbound           Outbound manual security association
Please Input the code of command to be excute(0-1): 1
Key Word:
Q(quit)
(00)ah                 AH key
(01)esp                ESP key
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00)<256-4294967295>   SPI for security association
Please Input the code of command to be excute(0-0): 0
Please input a digital number:20000 (Input SPI Value)
Key Word:
Q(quit)
(00)WORD                security association key value (hex w/o leading 0x)
Please Input the code of command to be excute(0-0): 0
Please input a string:654321 (input security association key value )
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(05)english            help message in English
(06)exit                exit / quit
.....
Please Input the code of command to be excute(0-19): 6
Will you excute it? (Y/N):y

```

Repeat these steps to create additional crypto map entries as required.

### Creat Crypto Map Entries that Used IKE

To create crypto map entries that will use IKE to establish the security associations, use the following commands starting in global configuration mode:

| Step | Command                                                          | Purpose                                                                                                                                                                                                     |
|------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>crypto map</b> <i>map-name seq-num</i><br><b>ipsec-isakmp</b> | Specifies the crypto map entry to create (or modify). Perform this command into the crypto map configuration mode.                                                                                          |
| 2    | <b>Match address</b> <i>access-list-name</i>                     | Configure an IPSec access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry. |
| 3    | <b>set peer</b> <i>ip-address</i>                                | Specifies the address of IPSec peer. This is the address to which IPSec protected traffic should be forwarded.                                                                                              |
| 4    | <b>set transform-set</b> <i>transform-set-name1</i>              | Configure transform sets. No more than six crypto map                                                                                                                                                       |

|   |                                                                                                                                             |                                                                                                                                                                                                            |
|---|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | [ <i>transform-set-name2...transform-set-name6</i> ]                                                                                        | entries can be specified (highest priority first).                                                                                                                                                         |
| 5 | <b>set security-association lifetime seconds</b><br><i>seconds</i> 或 <b>set security-association lifetime kilobytes</b><br><i>kilobytes</i> | (Optional) Specifies a security association lifetime for the crypto map entry.                                                                                                                             |
| 6 | <b>set pfs [group1   group2]</b>                                                                                                            | (Optional) Specifies that IPsec should ask for perfect forward secrecy when requesting new security associations for this crypto map entry, or should demand PFS in requests received from the IPsec peer. |
| 7 | <b>exit</b>                                                                                                                                 | Exits crypto-map configuration mode and return to global configuration mode.                                                                                                                               |

```
DEFAULT@Router /config/]#crypto
```

```
Key Word:
```

```
U(undo) D(default) Q(quit)
```

```
.....
```

```
(02)isakmp Configure ISAKMP policy
```

```
(03)map Enter a crypto map
```

```
Please Input the code of command to be excute(0-3): 3
```

```
Key Word:
```

```
Q(quit)
```

```
(00)WORD Crypto map name
```

```
Please Input the code of command to be excute(0-0): 0
```

```
Please input a string:abc (Input Crypto map name)
```

```
Key Word:
```

```
Q(quit)
```

```
(00)<0-65535> Sequence to insert into crypto map entry
```

```
(01)local-address Interface to use for local address for this crypto map
```

```
Please Input the code of command to be excute(0-1): 0
```

```
Please input a digital number:123 (Input Sequence Value)
```

```
Key Word:
```

```
Q(quit)
```

```
(00)ipsec-isakmp IPSEC w/ISAKMP
```

```
(01)ipsec-manual IPSEC w/manual keying
```

```
Please Input the code of command to be excute(0-1): 0
```

```
Key Word:
```

```
Q(quit)
```

```
(00)dynamic Enable dynamic crypto map support
```

```
(01)<cr>
```

```
Please Input the code of command to be excute(0-1): 1
```

```
Will you excute it? (Y/N):y
```

```
Key Word:
```

```
Q(quit)
```

```
.....
```

```
(10)interface interface configuration
```

```
(11)match Match values
```

```
.....
```

```
Please Input the code of command to be excute(0-19): 11
```

```
Key Word:
```

```
U(undo) D(default) Q(quit)
```

```
(00)address Match address of packets to encrypt.
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)WORD Access-list name
Please Input the code of command to be excute(0-0): 0
Please input a string:list1 (Input Access-list name)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(16)set Set values for encryption/decryption
(17)show show configuration and status
.....
Please Input the code of command to be excute(0-19): 16
Key Word:
U(undo) D(default) Q(quit)
(00)peer Allowed Encryption/Decryption peer.
(01)pfs Specify pfs settings
.....
Please Input the code of command to be excute(0-3): 0
Key Word:
Q(quit)
(00)A.B.C.D IP address of peer
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:10.0.0.2 (input peer ip address)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(15)router routing protocol configuration
(16)set Set values for encryption/decryption
.....
Please Input the code of command to be excute(0-19): 16
Key Word:
U(undo) D(default) Q(quit)
.....
(02)security-association Security association parameters
(03)transform-set Specify list of transform sets
Please Input the code of command to be excute(0-3): 3
Key Word:
Q(quit)
(00)WORD transform-set name
Please Input the code of command to be excute(0-0): 0
Please input a string:ts-1
Key Word:
Q(quit)
(00)WORD transform-set name
(01)<CR>
```

```

Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(15)router          routing protocol configuration
(16)set             Set values for encryption/decryption
.....
Please Input the code of command to be excute(0-19): 16
Key Word:
U(undo) D(default)      Q(quit)
.....
(02)security-association Security association parameters
(03)transform-set       Specify list of transform sets
Please Input the code of command to be excute(0-3): 2
Key Word:
Q(quit)
(00)lifetime          security association lifetime
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)kilobytes         Volume-based key duration
(01)seconds           Time-based key duration
Please Input the code of command to be excute(0-1): 1
Key Word:
Q(quit)
(00)<120-86400>       Security association duration in seconds
Please Input the code of command to be excute(0-0): 0
Please input a digital number:500 (input duration value)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(15)router          routing protocol configuration
(16)set             Set values for encryption/decryption
.....
Please Input the code of command to be excute(0-19): 16
Key Word:
U(undo) D(default)      Q(quit)
(00)peer             Allowed Encryption/Decryption peer.
(01)pfs              Specify pfs settings
.....
Please Input the code of command to be excute(0-3): 1
Key Word:
Q(quit)
(00)group1           D-H Group1
(01)group2           D-H Group2
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y

```

```

Key Word:
Q(quit)
.....
(05)english                help message in English
(06)exit                   exit / quit
.....
Please Input the code of command to be excute(0-19): 6
Will you excute it? (Y/N):y

```

Repeat these steps to create additional crypto map entries as required.

#### 6.4.4.5 Apply Crypto Map Sets To Interfaces

You need to apply a crypto map set to each interface through which IPSec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto.

To apply a crypto map set to an interface, use the following command in interface configuration mode:

| Command                           | Purpose                                   |
|-----------------------------------|-------------------------------------------|
| <b>crypto map</b> <i>map-name</i> | Applies a crypto map set to an interface. |

```

Key Word:
Q(quit)
.....
(04)clear_drv              clear interface statistic counter
(05)crypto                 Encryption module
.....
Please Input the code of command to be excute(0-34): 5
Key Word:
U(undo) D(default)       Q(quit)
(00)map                   Assign a crypto map
Please Input the code of command to be excute(0-0): 0
Key Word:
Q(quit)
(00)WORD                  Crypto map name
Please Input the code of command to be excute(0-0): 0
Please input a string:abc (input Crypto map name)
Will you excute it? (Y/N):y

```

Apply the same crypto map set to more than one interface.

#### 6.4.5 IPSec Configuration Example

The following example shows a minimal IPSec configuration where the security associations will be established via IKE.

For more information about IKE, see the "[Configure IKE](#)" chapter.

Define an IPSec access list:

```

config-ip access-list extended aaa
config-permit ip 130.130.0.0 255.255.0.0 131.131.0.0 255.255.0.0

```

Define transform set:

```

crypto ipsec transform-set one
config transform-type esp-des esp-sha-hmac

```

A crypto map specifies the IPSec access list and transform set and specifies where the protected traffic is sent (the IPSec

peer):

```
crypto map toShanghai 100 ipsec-isakmp
config-address aaa
set transform-set one
set peer 192.2.2.1
```

The crypto map is applied to an interface:

```
config-interface Serial0/0
config-ip addr192.2.2.2
crypto map toShanghai
```

## 6.5 Configuring Internet Key Exchange Security Protocol

### 6.5.1 Overview

This chapter describes how to configure the Internet Key Exchange (IKE) protocol. IKE is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and the Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

### 6.5.2 About IKE

IKE automatically negotiates IPSec security associations (SA) and enables IPSec secure communications without costly manual preconfiguration. IKE provides these benefits:

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- Allows you to specify a lifetime for the IPSec security association.
- Allows encryption keys to change during IPSec sessions.
- Allows IPSec to provide anti-replay services.
- Allows dynamic authentication of peers.

#### Supported Standards

The Router implements the following standards:

**IPSec**—IP Security Protocol. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**Internet Key Exchange (IKE)**—A hybrid protocol which implements Oakley and Skeme key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

**SAKMP**—The Internet Security Association and Key Management Protocol. A protocol framework which defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

**Oakley**—A key exchange protocol which defines how to derive authenticated keying material.

**Skeme**—A key exchange protocol which defines how to derive authenticated keying material, with rapid key refreshment.

The component technologies implemented for use by IKE include:

DES—The Data Encryption Standard.

3DES—Triple DES (3DES) utilize to packet-data encryption.

Diffie-Hellman—A public-key cryptography protocol which allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported.

MD5 (HMAC variant)—MD5 (Message Digest 5) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.

SHA (HMAC variant)—SHA (Secure Hash Algorithm) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing

### 6.5.3 Terms

Security association

Anti-replay

Perfect forward secrecy (PFS)

Data authentication

## 6.5.4 IKE Configuration Steps

To configure IKE, perform the tasks in the following sections. The tasks in the first three sections are required; the remaining may be optional, depending on what parameters are configured.

Ensure Access Lists Are Compatible with IKE

Create IKE Policies

Configure Pre-Shared Keys

Clear IKE Connections (optional)

Troubleshoot IKE (Optional)

For IKE configuration examples, refer to the "[IKE Configuration Example](#)" section located at the end of this chapter.

### **Ensure Access Lists Are Compatible with IKE**

IKE negotiation uses UDP on port 500. Ensure that your access lists are configured so that UDP port 500 traffic is not blocked at interfaces used by IKE and IPSec. In some cases you might need to add a statement to your access lists to explicitly permit UDP port 500 traffic.

### **Create IKE Policies**

You must create IKE policies at each peer. An IKE policy defines a combination of security parameters to be used during the IKE negotiation.

To create an IKE policy, follow the guidelines in these sections:

Why Do You Need to Create These Policies

What Parameters Do You Define in a Policy

How Do IKE Peers Agree upon a Matching Policy

Which Value Should You Select for Each Parameter

Creating Policies

Additional Configuration Required for IKE Policies

### **Why Do You Need to Create These Policies**

IKE negotiations must be protected, so each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations.

After the two peers agree upon a policy, the security parameters of the policy are identified by a security association established at each peer, and these security associations apply to all subsequent IKE traffic during the negotiation.

You must create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer's policy.

### What Parameters Do You Define in a Policy

There are five parameters to define in each IKE policy:

| Parameter                       | Accepted Values                                                    | Keyword                          | Default Value            |
|---------------------------------|--------------------------------------------------------------------|----------------------------------|--------------------------|
| encryption algorithm            | 56-bits DES-CBC<br>168-bits 3DES-CBC                               | des<br>3des                      | 56-bits DES-CBC          |
| hash algorithm                  | SHA-1<br>MD5                                                       | sha<br>md5                       | SHA-1                    |
| authentication method           | pre-shared keys<br>RSA signatures<br>RSA encrypted nonces          | pre-share<br>rsa-sig<br>rsa-encr | pre-shared keys          |
| Diffie-Hellman group identifier | 768 bytes Diffie-Hellman<br>1024 bytes Diffie-Hellman              | 1<br>2                           | 768 bytes Diffie-Hellman |
| security association's lifetime | can specify any number of seconds from 60 seconds to 86400 seconds | -                                | 86400 second (one day)   |

### How Do IKE Peers Agree upon a Matching Policy

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared.

If no acceptable match is found, IKE refuses negotiation and IPSec will not be established.

If a match is found, IKE will complete negotiation, and IPSec security associations will be created.

**Note: Depending on which authentication method is specified in a policy, additional configuration might be required**

### Which Value Should You Select for Each Parameter

The encryption algorithm has two options: 56-bit DES-CBC and 168-bits 3DES-CBS, the latter is more security. .

The hash algorithm has two options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a demonstrated successful (but extremely difficult) attack against MD5; however, the HMAC variant used by IKE prevents this attack.

The authentication method has three options: RSA signatures, RSA encrypted nonces, and pre-shared keys. Currently only pre-shared keys are supported.

The Diffie-Hellman group identifier has two options: 768-bit or 1024-bit Diffie-Hellman. 1024-bit Diffie-Hellman is harder to crack, but requires more CPU time to execute.

The security association's lifetime can be set to any value. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPSec security associations can be set up more quickly. For more information about this parameter and how it is used, see the command description for the **lifetime (IKE policy)** command.

### Creating Policies

You can create multiple IKE policies, each with a different combination of parameter values. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).

You can configure multiple policies on each peer—but at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer.

If you do not configure any policies, your router will use the default policy, which is always set to the lowest priority, and which contains each parameter's default value.

To configure a policy, use the following commands starting in global configuration mode:

| Step | Command                                                 | Purpose                                                                                                                                                |
|------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>crypto isakmp policy</b> <i>priority</i>             | Create IKE policy (Each policy is uniquely identified by the priority number you assign.) (This command puts you into the config-isakmp command mode.) |
| 2    | <b>encryption</b> {des 3des}                            | Specify the encryption algorithm.                                                                                                                      |
| 3    | <b>hash</b> {sha   md5}                                 | Specify the hash algorithm.                                                                                                                            |
| 4    | <b>authentication</b><br>{ pre-share rsa-sig rsa-encr } | Specify the authentication method.                                                                                                                     |
| 5    | <b>group</b> { 1   2 }                                  | Specify the Diffie-Hellman group.                                                                                                                      |
| 6    | <b>lifetime</b> <i>seconds</i>                          | Specify the security association's lifetime.                                                                                                           |
| 7    | <b>Exit</b>                                             | Exit the config-isakmp command mode.                                                                                                                   |
| 8    | <b>show crypto isakmp policy</b>                        | (Optional) View all existing IKE policies. (Use this command in EXEC mode.)                                                                            |

```
[DEFAULT@Router /config/]#crypto
```

```
Key Word:
```

```
U(undo) D(default) Q(quit)
```

```
.....
```

```
(02)isakmp Configure ISAKMP policy
```

```
(03)map Enter a crypto map
```

```
Please Input the code of command to be excute(0-3): 2
```

```
Key Word:
```

```
Q(quit)
```

```

(00)key                Set pre-shared key for remote peer
(01)policy             Set policy for an ISAKMP protection suite
Please Input the code of command to be excute(0-1): 1
Key Word:
Q(quit)
(00)<1-10000>         Priority of protection suite
Please Input the code of command to be excute(0-0): 0
Please input a digital number:10 (Input Priority Value)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(06)encryption        Set encryption algorithm for protection suite
(07)english           help message in English
.....
Please Input the code of command to be excute(0-22): 6
Key Word:
U(undo) D(default)   Q(quit)
(00)des              Data Encryption Standard
(01)3des             Triple Data Encryption Standard
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(10)hash             Set hash algorithm for protection suite
(11)help            Description of the interactive help system
.....
Please Input the code of command to be excute(0-22): 10
Key Word:
U(undo) D(default)   Q(quit)
(00)md5             Message Digest 5
(01)sha             Secure Hash Standard
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y
Key Word:
Q(quit)
(00)authentication  Set authentication method for protection suite
(01)chinese         help message in Chinese
(02)chmem          Change memory of system
.....
Please Input the code of command to be excute(0-22): 0
Key Word:
U(undo) D(default)   Q(quit)
(00)pre-share       Pre-Shared Key
Please Input the code of command to be excute(0-0): 0
Will you excute it? (Y/N):y
Key Word:
Q(quit)

```

```

.....
(08)exit                exit / quit
(09)group                Set the Diffie-Hellman group
.....
Please Input the code of command to be excute(0-22): 9
Key Word:
U(undo) D(default)      Q(quit)
(00)<1-2>                group description number
Please Input the code of command to be excute(0-0): 0
Please input a digital number:1 (Input group description number)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(15)lifetime            Set lifetime for ISAKMP security association
(16)no                  negate configuration
.....
Please Input the code of command to be excute(0-22): 15
Key Word:
U(undo) D(default)      Q(quit)
(00)<60-86400>           lifetime in seconds
Please Input the code of command to be excute(0-0): 0
Please input a digital number:500 (Input lifetime in seconds)
Will you excute it? (Y/N):y
Key Word:
Q(quit)
.....
(08)exit                exit / quit
(09)group                Set the Diffie-Hellman group
.....
Please Input the code of command to be excute(0-22): 8
Will you excute it? (Y/N):y
[DEFAULT@Router /config/]#show
Key Word:
U(undo) D(default)      Q(quit)
.....
(09)cpu                 cpu usage information
(10)crypto              Encryption module
.....
Please Input the code of command to be excute(0-50): 10
Key Word:
Q(quit)
(00)dynamic-map         Crypto map templates
(01)ipsec               Show IPSEC policy
(02)isakmp              Show ISAKMP Security Association
(03)map                 Crypto map
Please Input the code of command to be excute(0-3): 2
Key Word:
Q(quit)

```

```
(00)policy          Show ISAKMP protection suite policy
(01)sa              Show ISAKMP Security Associations
Please Input the code of command to be excute(0-1): 0
Will you excute it? (Y/N):y
```

If you do not specify a value for a parameter, the default value is assigned.

Note: The default policy and the default values for configured policies do not show up in the configuration when you issue a show running command. Instead, to see the default policy and any default values within configured policies, use the show crypto isakmp policy command.

### Additional Configuration Required for IKE Policies

Pre-shared keys authentication method: If you specify pre-shared keys as the authentication method in a policy, you must configure these pre-shared keys.

### Configure Pre-Shared Keys

To specify the shared keys at IPSec each peer. Note that a given pre-shared key is shared between two peers. At each peer you could specify the same key.

To specify pre-shared keys at a peer, use the following commands in global configuration mode:

| Step | Command                                                             | Purpose                                                                                    |
|------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1    | <code>crypto isakmp key <i>keystring</i> <i>peer-address</i></code> | <b>At the local peer:</b> Specify the shared key to be used with a particular remote peer. |
| 2    | <code>crypto isakmp key <i>keystring</i> <i>peer-address</i></code> | <b>At the remote peer:</b> Specify the shared key to be used with the local peer.          |

```
[DEFAULT@Router /config/]#crypto
Key Word:
U(undo)          D(default)          Q(quit)
(00)dynamic-map  Specify a dynamic crypto map template
(01)ipsec        Configure IPSEC policy
(02)isakmp       Configure ISAKMP policy
(03)map          Enter a crypto map
Please Input the code of command to be excute(0-3): 2
Key Word:
Q(quit)
(00)key          Set pre-shared key for remote peer
(01)policy       Set policy for an ISAKMP protection suite
Please Input the code of command to be excute(0-1): 0
Key Word:
Q(quit)
(00)WORD         pre-shared key
Please Input the code of command to be excute(0-0): 0
Please input a string:123
Key Word:
Q(quit)
(00)A.B.C.D      shared key IP address
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:192.168.0.1 (Input IP address)
```

Will you excute it? (Y/N):y

### Clear IKE Connection (optional)

If you want, you can clear existing IKE connections. To clear IKE connections, use the following commands in EXEC mode:

| Step | Command                                                     | Purpose                 |
|------|-------------------------------------------------------------|-------------------------|
| 1    | <b>show crypto isakmp sa</b>                                | View existing isakmp SA |
| 2    | <b>clear crypto isakmp [map map-name   peer ip-address]</b> | Clear isakmp connection |

```
[DEFAULT@Router /enable/]#show
```

```
Key Word:
```

```
U(undo) D(default) Q(quit)
```

```
.....
```

```
(09)cpu cpu usage information
```

```
(10)crypto Encryption module
```

```
.....
```

```
Please Input the code of command to be excute(0-50): 10
```

```
Key Word:
```

```
Q(quit)
```

```
.....
```

```
(02)isakmp Show ISAKMP Security Association
```

```
(03)map Crypto map
```

```
Please Input the code of command to be excute(0-3): 2
```

```
Key Word:
```

```
Q(quit)
```

```
(00)policy Show ISAKMP protection suite policy
```

```
(01)sa Show ISAKMP Security Associations
```

```
Please Input the code of command to be excute(0-1): 1
```

```
Will you excute it? (Y/N):y
```

```
[DEFAULT@Router /enable/]#clear
```

```
Key Word:
```

```
U(undo) D(default) Q(quit)
```

```
(00)arp-cache Clear the entire ARP cache
```

```
(01)crypto Encryption module
```

```
.....
```

```
Please Input the code of command to be excute(0-15): 1
```

```
Key Word:
```

```
Q(quit)
```

```
(00)isakmp Flush the ISAKMP database
```

```
(01)sa Clear all crypto SAs
```

```
Please Input the code of command to be excute(0-1): 0
```

```
Key Word:
```

```
Q(quit)
```

```
(00)map Clear all isakmp SAs for a given crypto map
```

```
(01)peer Clear all isakmp SAs for a given crypto peer
```

```
(02)<cr>
```

```
Please Input the code of command to be excute(0-2): 1
```

```
Key Word:
```

```

Q(quit)
(00)A.B.C.D                      Crypto peer address
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:192.168.0.1 (Input ip address)
Will you excute it? (Y/N):y

```

### Troubleshoot IKE (optional)

To assist in IKE troubleshooting, use the following commands in EXEC mode:

| Command                          | Purpose                                             |
|----------------------------------|-----------------------------------------------------|
| <b>show crypto isakmp policy</b> | View the parameters for each configured IKE policy. |
| <b>show crypto isakmp sa</b>     | View all current IKE security associations.         |
| <b>debug crypto isakmp</b>       | Display <b>debug</b> messages about IKE events.     |

```

[DEFAULT@Router /enable/]#show
Key Word:
U(undo) D(default)      Q(quit)
.....
(09)cpu                  cpu usage information
(10)crypto               Encryption module
.....
Please Input the code of command to be excute(0-50): 10
Key Word:
Q(quit)
.....
(02)isakmp              Show ISAKMP Security Association
(03)map                  Crypto map
Please Input the code of command to be excute(0-3): 2
Key Word:
Q(quit)
.....
(00)policy              Show ISAKMP protection suite policy
(01)sa                  Show ISAKMP Security Associations
Please Input the code of command to be excute(0-1): 0 (Select 0 or 1 when necessary)
Will you excute it? (Y/N):y

```

### 6.5.5 What To Do Next

After IKE configuration is complete, you can configure IPsec. IPsec configuration is described in the "Configuring IPsec" chapter.

### 6.5.6 IKE Configuration Examples

This example creates two IKE policies, with policy 10 as the highest priority, policy 20 as the next priority and the existing default priority as the lowest priority. it also creates a pre-shared key to be used with the remote policies whose IP address is 192.168.1.3.

```

crypto isakmp policy 10
encryption des
hash md5

```

```
authentication pre-share
group 2
lifetime 5000
crypto isakmp policy 20
authentication pre-share
lifetime 10000
crypto isakmp key 1234567890 192.168.1.3
```

In the above example, **encryption des** of policy 10 would not appear in the written configuration because this is the default value for the encryption algorithm parameter.

If the **show crypto isakmp policy** command is issued with this configuration, the output would be as follows:

Protection suite of priority 10

```
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group:  #1 (768 bit)
lifetime:              5000 seconds
```

Protection suite of priority 20

```
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group:  #1 (768 bit)
lifetime:              10000 seconds
```

Default protection suite

```
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group:  #1 (768 bit)
lifetime:              86400 seconds
```

## 7. QoS Configuration

This chapter explains what is Quality of Service (QoS for short), and the service models that fulfill it. Moreover, introduce queue algorithms of QoS. The relating configuration please refer to QoS Configuration.

### 7.1 QoS Overview

#### QoS Overview

This chapter explains quality of service (QoS) and the service models that embody it. In addition, QoS Queue Algorithm will be introduced. For the correlative configuration, see the [QoS Configuration](#).

#### 7.1.1 What is QoS

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, ATM (Asynchronous Transfer Mode), Ethernet and 802.1 networks, and IP-routed networks. In command to ensure the QoS in the network, the Router provides queueing, scheduling, and QoS signalling features. The Router features enable networks to control and predictably service a variety of networked applications and traffic types.

#### 7.1.2 End-to-End QoS Models

A service model, also called a level of service, describes a set of end-to-end QoS capabilities. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. The QoS software supports three types of service models: best effort, integrated, and differentiated services.

##### 7.1.2.1 Best-Effort Service

Best effort is a single service model in which an application sends data whenever it must, in any quantity, and without requesting permission or first informing the network. For best-effort service, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. The QoS feature that implements best-effort service is FIFO queueing.

##### 7.1.2.2 Integrated Service

Integrated service is a multiple service model that can accommodate multiple QoS requirements. In this model the application requests a specific kind of service from the network before it sends data. The request is made by explicit signalling; the application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. It is also expected to send data that lies within its described traffic profile.

The network performs admission control, based on information from the application and available network resources. It also commits to meeting the QoS requirements of the application as long as the traffic remains within the profile specifications.

The QoS provide Controlled Load Service and Guaranteed Rate Service by the Resource Reservation Protocol (RSVP). Controlled Load Service, which allows applications to have low delay and high throughput even during times of congestion. D-Link QoS uses Weighted Fair Queueing ([WFQ](#)) to provide this kind of service..

##### 7.1.2.3 Differentiated Service

Differentiated service is a multiple service model that can satisfy differing QoS requirements. However, unlike in the integrated service model, an application using differentiated service does not explicitly signal the router before sending data.

For differentiated service, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the IP Precedence bit settings in IP packets or source and destination addresses. The router uses the QoS specification to classify and to perform intelligent queueing.

The QoS provides Weighted Random Early Detection ([WRED](#)), Custom Queueing ([CQ](#)), and Priority Queueing ([PQ](#)) to deliver differentiated services.

### 7.1.3 QoS Queueing Algorithms

QoS Queueing Algorithms are the important guarantee to achieve QoS configuration. D-LINK router supports Weighted Fair Queueing ([WFQ](#)), Custom Queueing ([CQ](#)), Priority Queueing ([PQ](#)), Weighted Random Early Detection ([WRED](#)), and the simplest first-in and first-out (FIFO) algorithm.

#### 7.1.3.1 Weighted Fair Queueing

WFQ is a dynamic scheduling method that provides fair bandwidth allocation to all network traffic. WFQ applies priority, or weights, to identified traffic to classify traffic into conversations and determine how much bandwidth each conversation is allowed relative to other conversations. WFQ is a flow-based algorithm that simultaneously schedules interactive traffic to the front of a queue to reduce response time and fairly shares the remaining bandwidth among high-bandwidth flows. In other words, WFQ allows you to give low-volume traffic, such as Telnet sessions, priority over high-volume traffic, such as FTP sessions. WFQ gives concurrent file transfers balanced use of link capacity; that is, when multiple file transfers occur, the transfers are given comparable bandwidth.

WFQ overcomes a serious limitation of FIFO queueing. When FIFO is in effect, traffic is sent in the order received without regard for bandwidth consumption or the associated delays. As a result, file transfers and other high-volume network applications often generate series of packets of associated data and depriving other traffic of bandwidth. WFQ provides traffic priority management that dynamically sorts traffic into messages that make up a conversation to ensure that bandwidth is shared fairly between individual conversations and that low-volume traffic is transferred in a timely fashion.

WFQ classifies traffic into different flows based on packet header addressing. For most of traffic are IP data, thus the WFQ classifies the data packets based on characteristics of IP header, including such characteristics as source and destination address, source and destination port, protocol types, and ToS value.

WFQ places packets of the various conversations in the fair queues before transmission. The order of removal from the fair queues is determined by the virtual time of the delivery of the last bit of each arriving packet (finish number).

Flow-based WFQ is used as the default queueing mode on most serial interfaces configured to run at E1 speeds (2.048 Mbps) or below.

See the [WFQ Configuration](#) for particular configuration of WFQ.

WFQ is only automatically identify flow but does not offer the special service for some peculiar flow. D-Link router provides Class-Based Weighted Fair Queueing (CBWFQ), which enhanced the standard WFQ. It can identifies the type of flow by user customization and distribute the authority to the flow.

See the [CBWFQ Configuration](#) for particular configuration of CBWFQ.

#### 7.1.3.2 Weighted Random Early Detection

Random Early Detection (RED) is a common congestion avoidance mechanism. Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic. However, you can also configure WRED to ignore IP precedence when making drop decisions so that non-weighted RED behavior is achieved.

WRED is useful on any output interface where you expect to have congestion. However, WRED is usually used in the core routers of a network, rather than the edge. Edge routers assign IP precedences to packets as they enter the network. WRED uses these precedences to determine how it treats different types of traffic.

When RED is not configured, output buffers fill during periods of congestion. When the buffers are full, tail drop occurs; all additional packets are dropped. Since the packets are dropped all at once, global synchronization of TCP hosts can occur as multiple TCP hosts reduce their transmission rates. The congestion clears, and the TCP hosts increase their transmissions rates, resulting in waves of congestion followed by periods where the transmission link is not fully used.

RED reduces the chances of tail drop by selectively dropping packets when the output interface begins to show signs of congestion. By dropping some packets early rather than waiting until the buffer is full, RED avoids dropping large numbers of packets at once and minimizes the chances of global synchronization. Thus, RED allows the transmission line to be used fully at all times.

In addition, RED statistically drops more packets from large users than small. Therefore, traffic sources that generate the most traffic are more likely to be slowed down than traffic sources that generate little traffic.

WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service for different traffic. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

See the [WRED Configuration](#) for concrete configuration.

### 7.1.3.3 Custom Queueing

When CQ is enabled on an interface, the system maintains 17 output queues for that interface. You can specify queues 1 through 16. Associated with each output queue is a configurable byte count, which specifies how many bytes of data the system should deliver from the current queue before it moves on to the next queue.

Queue number 0 is a system queue; it is emptied before any of the queues numbered 1 through 16 are processed. The system queues high priority packets, such as keepalive packets and signalling packets, to this queue. Other traffic cannot be configured to use this queue.

For queue numbers 1 through 16, the system cycles through the queues sequentially (in a round-robin fashion), dequeuing the configured byte count from each queue in each cycle, delivering packets in the current queue before moving on to the next one. When a particular queue is being processed, packets are sent until the number of bytes sent exceeds the queue byte count or the queue is empty. Bandwidth used by a particular queue can only be indirectly specified in terms of byte count and queue length. Like PQ, CQ is statically configured and does not automatically adapt to changing network conditions

See the [CQ Configuration](#) for concrete configuration.

### 7.1.3.4 Priority Queueing

PQ define 4 class of communication priority(high,middle,normal,low). During transmission, PQ gives priority queues absolute preferential treatment over low priority queues; important traffic, given the highest priority, always takes precedence over less important traffic.

Packets are classified based on user-specified criteria and placed into one of the four output queues—high, medium, normal, and low—based on the assigned priority. Packets that are not classified by priority fall into the normal queue. When a packet is to be sent out an interface, the priority queues on that interface are scanned for packets in descending command of priority. The high priority queue is scanned first, then the medium priority queue, and so on. The packet at the head of the highest queue is chosen for transmission. This procedure is repeated every time a packet is to be sent.

See the [PQ Configuration](#) for concrete configuration.

### 7.1.4 QoS Signalling

The Router QoS signalling provides a way for an end station or network node to signal its neighbors to request special handling of certain traffic. QoS signalling is useful for coordinating the traffic handling techniques provided by other QoS features. It plays a key role in configuring successful overall end-to-end QoS service across your network. QoS signalling takes advantage of IP. Either in-band (IP Precedence, 802.1p) or out-of-band (RSVP) signalling is used to indicate that a particular QoS service is desired for a particular traffic classification. Together, IP Precedence and RSVP provide a robust combination for end-to-end QoS signalling: IP Precedence signals for differentiated QoS and RSVP for guaranteed QoS.

For more complete conceptual information, see the chapter "Resource Reservation Protocol (RSVP)"

### 7.1.5 QoS Link Efficiency Mechanisms

The Router offers Compressed Real-Time Protocol (CRTP) mechanism to improve efficiency of the bandwidth. See to related CRTP references for information.

## 7.2 Configure QoS

### QoS Configuration Overview

Before configuring QoS, you must configure queueing algorithm, QoS signaling and QoS link efficiency mechanisms. The last two are optional and the first one has the default value which can be altered according to the instances on every interface.

### 7.2.1 QoS Queueing Configuration

#### 7.2.1.1 Configure WFQ

To configure fair queueing on an interface, use one of the following commands in interface configuration mode after specifying the interface:

| Command           | Purpose                                      |
|-------------------|----------------------------------------------|
| <b>fair-queue</b> | Configure an interface to use fair queueing. |

[DEFAULT@Router /config/]#**interface**

Key Word:

U(undo) D(default) Q(quit)  
 (00)FastEthernet   FastEthernet interface  
 (01)Ethernet        Ethernet interface  
 (02)Serial           Serial interface  
 (03)Async           Asynchronous interface  
 (04)Null            Null interface  
 (05)Loopback        Loopback interface  
 (06)Tunnel           Tunnel interface  
 (07)Dialer           Dialer interface

- (08)Multilink Multilink-group interface
- (09)Virtual-template Virtual template interface
- (10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): **0**

**Note** : Select an interface here, the FastEthernet is only for example.

Please input a interface name:**f0/0**

**Note** : Input an interface here, the f0/0 is only for example

Will you excute it? (Y/N): y

Key Word:

Q(quit)

- (00)arp set arp timeout
- (01)backup Modify backup parameters
- (02)bandwidth Set the interface bandwidth
- (03)bridge-group Transparent bridging interface parameters
- (05)chinese help message in Chinese
- (06)chmem Change memory of system
- (07)clear\_drv clear interface statistic counter
- (08)crypto Encryption module
- (09)custom-queue-list Assign a custom queue list to interface
- (10)default restore default configuration
- (11)delay Set the interface delay
- (12)description Set the interface description
- (13)duplex Configure duplex operational mode
- (14)english help message in English
- (15)exit exit / quit
- (16)fair-queue enable fair queue on interface
- (17)help Description of the interactive help system
- (18)history look up history
- (19)interface interface configuration
- (20)ip IP configuration commands
- (21)keepalive Enable keepalive
- (22)llc2 Setup LLC2(Logic Link Control Type2) parameters
- (23)no negate configuration
- (24)pdp pdp configuration commands
- (25)physical-interface Configure lan physical interface
- (26)pppoe-client pppoe client enable
- (27)priority-group Assign a priority group to interface
- (29)random-detect enable weighted random early detect on interface
- (30)router routing protocol configuration
- (31)service-policy Assign a priority group to interface
- (32)show show configuration and status
- (33)shutdown Shutdown the current interface
- (34)snmp Modify SNMP interface parameters
- (35)speed Configure speed operation

Please Input the code of command to be excute(0-35): **16 ( select fair-queue )**

Will you excute it? (Y/N):y

Note: WFQ is the default queueing mode on interfaces that run at or below E1 speeds (2.048 Mb/s or less). It is enabled by default for physical interfaces that do not use Link Access Procedure Balanced (LAPB) or X.25 encapsulations.

## 7.2.1.2 Configure Policy Map On An Interface (CBWFQ)

After configure a policy map, CBWFQ will take effect on the interface. To configure a policy map on the interface which you have specified, you can use the following commands in interface configuration mode:

| Command                                  | Purpose                                               |
|------------------------------------------|-------------------------------------------------------|
| <b>service-policy</b> <i>policy-name</i> | specifying the interface using command set-policy-map |

Select **service-policy** command in the directory of configure interface

Key Word:

U(undo) D(default) Q(quit)

(00)WORD policy-map name

Please Input the code of command to be excute(0-0): **0**

Input 0 to select WORD option, input policy map name at prompt:

Please input a string:**name**

**Note** : Input the policy map name here, name is only for example.

Will you excute it? (Y/N):**y**

**Note** : **This command is only available in the interfaces that have configured WFQ algorithm.**

Configure Policy Map

By configuring the policy map and the class map that embodied in it, a group of flow with different type can be specified. When an interface uses the policy map, certain QoS can be ensured according to the specified flow type.

In command to configure policy map, you need enter policy map configuration mode by using the command below in global configuration mode:

| Command                              | Purpose                                                      |
|--------------------------------------|--------------------------------------------------------------|
| <b>policy-map</b> <i>policy-name</i> | enter policy map configuration mode to configure policy map. |

[DEFAULT@Router /config/]#**policy-map**

Key Word:

U(undo) D(default) Q(quit)

(00)WORD policy-map name

Please Input the code of command to be excute(0-0): **0**

Input 0 and select WORD option, input policy-map name at prompt:

Please input a string:**name**

Note: Input policy map name here, name is only for example.

Will you excute it? (Y/N):**y**

Enter the policy configuration directory and output the following optional parameters:

Key Word:

Q(quit)

(00)chinese help message in Chinese

(01)chmem Change memory of system

(02)class config class map in this policy-map

(03)connect Open a outgoing connection

(04)default restore default configuration

(05)disconnect Disconnect an existing outgoing network connection

(06)english help message in English

(07)exit exit / quit

(08)help Description of the interactive help system

(09)history look up history

(10)interface interface configuration

- (11)no negate configuration
- (13)resume Resume an active outgoing network connection
- (14)router routing protocol configuration
- (15)show show configuration and status
- (16)telnet Open a telnet connection
- (17)where display all outgoing telnet connection

Please Input the code of command to be excute(0-17):

After entering policy map configuration mode, you can configure the class map name, bandwidth and the max number of the queues of the current policy map. In command to configure these, you can use the command below in policy map configuration mode:

| Command                                                                                         | Purpose                                                                                        |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| <b>class</b> class-name <b>bandwidth</b> bandwidth(kbps)<br>[ <b>queue-limit</b> packet-number] | Configure the bandwidth and the max number of the queues of a class map in current policy map. |

Input **2** , select **class**

Key Word:

U(undo) D(default) Q(quit)

(00)WORD class-map name

Please Input the code of command to be excute(0-0): **0**

Please input a string:**name**

**Note** : Input class map name here, name is only for example.

Key Word:

Q(quit)

(00)bandwidth specify bandwidth for this class-map

Please Input the code of command to be excute(0-0): **0**

(00)<8-2000000> Kilo Bits per second

Please Input the code of command to be excute(0-0): **0**

Please input a string:**100**

**Note** : Input bandwidth here, 100 is only for example.

Will you excute it? (Y/N):**y**

### Configure Class Map

By configuring t the class map, flow type can be specified. When an interface uses the policy map that embodies the class map, certain QoS can be ensured according to the specified flow type.

In command to configure class map, you can use the commands below in global configuration mode:

| Command                                                                                      | Purpose                                                |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------|
| <b>class-map</b> class-name <b>match protocol</b><br>protocol-type                           | Configuring a class map classified by protocol type.   |
| <b>class-map</b> class-name <b>match config-interface</b><br>interface-type interface-number | configuring a class map classified by interface type.  |
| <b>class-map</b> class-name <b>match access-group</b><br>list-name                           | Configuring a class map classified by access list type |

| Command                                                         | Purpose                                            |
|-----------------------------------------------------------------|----------------------------------------------------|
| <b>class-map</b> class-name <b>match protocol</b> protocol-type | Configure a class map classified by protocol types |

To configure the class map for the classification of protocol models, you can input:class-map:

```
[DEFAULT@Router /config/]#class-map
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)WORD      class-map name
```

Please Input the code of command to be excute(0-0): 0

Input 0, it will prompt to input the name of the class map, then displayed the following line:  
Please input a string:name

Note: Input a class map name, the name is only for example.

Key Word:

```
Q(quit)
(00)match      specify classification criteria
```

Please Input the code of command to be excute(0-0):0

Input 0, select the match option, then displayed the following line:

Key Word:

```
Q(quit)
(00)access-group  match a access-group
(01)protocol      match a protocol
(02)interface     match a input interface
```

Please Input the code of command to be excute(0-2): 1

Input 1, select protocol, and the Protocol menu displayed:

Key Word:

```
Q(quit)
(00)ip          internet protocol
(01)arp        Address Resolution Protocol
(02)comp_tcp   Compressed Tcp
```

Please Input the code of command to be excute(0-2): 2

Select a protocol model when necessary:

Will you excute it? (Y/N):y

Complete the class map for the classification of the protocol models:

| Command                                                                                          | Purpose                                                 |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>class-map</b> <i>class-name</i> <b>match interface</b> <i>interface-type interface-number</i> | Configure a class map classified by the interface types |

To configure the class map of the interface classification, please input: class-map:

```
[DEFAULT@Router /config/]#class-map
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)WORD      class-map name
```

Please Input the code of command to be excute(0-0): 0

it will prompt to input class map name, then display: Input 0

Please input a string:name

**Note** : Input class map name, name is only for example here.

Key Word:

```
Q(quit)
(00)match      specify classification criteria
```

Please Input the code of command to be excute(0-0):0

Input 0, select match option, then display: Input0

Key Word:

```
Q(quit)
```

- (00)access-group match a access-group
- (01)protocol match a protocol
- (02)interface match a input interface

Please Input the code of command to be excute(0-2): 2

Input 2, select interface, then displayed the interface option menu:

Key Word:

- Q(quit)
- (00)FastEthernet FastEthernet interface
- (01)Ethernet Ethernet interface
- (02)Serial Serial interface
- (03)Async Asynchronous interface

Please Input the code of command to be excute(0-3): 2

Select the interface model when needed, then input the interface name at prompt:

Please input a interface name:s2/0

Input the interface name

Will you excute it? (Y/N):y

Complete the class map for configuration interface classification.

| Command                                           | Purpose                                         |
|---------------------------------------------------|-------------------------------------------------|
| class-map class-name match access-group list-name | Configure a class map classified by access list |

To configure the class map of the interface classification, please input: class-map:

[DEFAULT@Router /config/#class-map

Key Word:

- U(undo) D(default) Q(quit)
- (00)WORD class-map name

Please Input the code of command to be excute(0-0): 0

It will prompt to input class map name, then display: Input 0

Please input a string:name

Note: Input class map name here, name is only for example.

Key Word:

- Q(quit)
- (00)match specify classification criteria

Please Input the code of command to be excute(0-0):0

select match option, then displayed: Input 0

Key Word:

- Q(quit)
- (00)access-group match a access-group
- (01)protocol match a protocol
- (02)interface match a input interface

Please Input the code of command to be excute(0-2): 0

Input 0, select access-group option, then displayed the access-group menu:

Key Word:

- Q(quit)
- (00)WORD IP access list name

Please Input the code of command to be excute(0-0): 0

Input 0, select WORD option and input the list name at prompt:

Please input a string:name

Note: Input the list name here, name is only for example.

Will you excute it? (Y/N):y

Here we completed the configuration of the class map of access list classification.

### 7.2.1.3 Configure WRED

If you need to configure a WRED on an interface, you can choose **random-detect** command under the global configuration directory after specifying the interface:

| Command                     | Purpose                        |
|-----------------------------|--------------------------------|
| <b>config-random-detect</b> | Applying WRED to an interface. |

Key Word:

Q(quit)

.....

- (27)priority-group Assign a priority group to interface
- (29)random-detect enable weighted random early detect on interface
- (30)router routing protocol configuration
- (31)service-policy Assign a priority group to interface
- (32)show show configuration and status
- (33)shutdown Shutdown the current interface
- (34)snmp Modify SNMP interface parameters
- (35)speed Configure speed operation

Please Input the code of command to be excute(0-35): **29** ( select random-detect )

Will you excute it? (Y/N):y

### 7.2.1.4 Configure CQ

If you want to configure CQ to an interface, you can use the command below in interface configuration mode after the interface specified:

| Command                                     | Purpose                                                                                                                                                                          |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>custom-queue-list</b> <i>list-number</i> | Applying CQ to the interface, <b>list-number</b> is the number of the adopted customed queue list. The list argument is any number from 1 to 16. There is no default assignment. |

If you need to configure a customed queue on more than one interfaces, you can select custom-queue-list in the interface commands under the directory of global configuration:

Key Word:

Q(quit)

- (00)arp set arp timeout
- (01)backup Modify backup parameters
- (02)bandwidth Set the interface bandwidth
- (03)bridge-group Transparent bridging interface parameters
- (05)chinese help message in Chinese
- (06)chmem Change memory of system
- (07)clear\_drv clear interface statistic counter
- (08)crypto Encryption module
- (09)custom-queue-list Assign a custom queue list to interface
- (10)default restore default configuration
- (11)delay Set the interface delay

.....

Please Input the code of command to be excute(0-35): **9** ( select custom-queue-list )

Will you excute it? (Y/N):**y**

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> Queue list number

Please Input the code of command to be excute(0-0): **0**

Select <1-16>option and input the list number Input0at prompt:

Please input a digital number::**1**

Note: Input 1-16 list numbers here, 1 is only for example.

Will you excute it? (Y/N):**y**

### Configuring Customed Queueing List

The customed queueing can define the custom queueing lists, and specify the approximate number of bytes to be forward and the total number of the queues. When applying the list to an interface, you can adjust the parameters according to the list.

To specify the total number of the queues and the approximate number of bytes to be forwarded, use one of the following commands in global configuration mode:

| Command                                                                                                          | Purpose                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>queue-list</b> <i>list-number</i> <b>queue</b> <i>queue-number</i> <b>limit</b> <i>limit-number</i>           | Specifies the maximum number of packets allowed in each of the custom queues. The <i>limit-number</i> argument specifies the number of packets that can be enqueued at any one time. The range is 0 to 32767.The default value is 20.  |
| <b>queue-list</b> <i>list-number</i> <b>queue</b> <i>queue-number</i> <b>byte-count</b> <i>byte-count-number</i> | Designates the number of bytes forwarded per queue. The <i>byte-count-number</i> argument specifies the min number of bytes the system allows to be delivered from a given queue during a particular cycle. The default value is 1500. |

To configure the upper limit of the CQ list, you can input in the global configuration list:

[DEFAULT@Router /config/#**queue-list**

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> Queue list number

Please Input the code of command to be excute(0-0): **0**

Input 0, select <1-16>option and it will prompt the following list:

Please input a digital number:**1**

**Note** : Input 1-16 list numbers here, 1 is only for example.

Key Word:

Q(quit)

(00)interface Establish priorities for packets from a named interface

(01)protocol Establish priorities for packets of a protocol

(02)queue configure parameters for a particular queue

(03)default set custom queue for unspecified packets

Please Input the code of command to be excute(0-3): **2**

Input 2 and select queue option:

Key Word:

Q(quit)

(00)<0-16> Queue number

Please Input the code of command to be excute(0-0): **0**

Input 0, select <1-16>option and it will prompt the queue menu:

Please input a digital number:1

**Note :** Input 1-16 queue number here, 1 is only for example.

Key Word:

Q(quit)

(00)byte-count specify size in bytes of a particular queue

(01)limit set queue max packets of a particular queue

Please Input the code of command to be excute(0-1): 1

Input 1, select <limit>option: (if you want to configure the customed list to send the byte numer, you can select the 0<byte-count>option)

Key Word:

Q(quit)

(00)<0-32767> Size in bytes

Please Input the code of command to be excute(0-0): 0

Input 0, select <0-32767>option, it will prompt to input the upper limit of the queue:

Please input a digital number:20

Input 20, it indicates that you have set 20 as the upper limit.

Key Word:

Q(quit)

(00)byte-count specify size in bytes of a particular queue

(01)<cr>

Please Input the code of command to be excute(0-1):1

Input 1

Will you excute it? (Y/N):y

You have completed configuring the upper limit of the queue list.

In the above example, if you input 0 and select<byte-count>, then it will continue to configure the customed list to send byte number, the following prompt displayed:

Key Word:

Q(quit)

(00)<1-16777215> Size in bytes

Please Input the code of command to be excute(0-0): 0

Input 0 and select the <1-16777215>option:

Please input a digital number:16

Key Word:

Q(quit)

(00)<cr>

Please Input the code of command to be excute(0-0): 0

Will you excute it? (Y/N):y

To define the custom queueing lists, use one of the following commands in global configuration mode:

| Command                                                                                                                              | Purpose                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>queue-list</b> <i>list-number</i> <b>protocol</b> <i>protocol-type</i><br><i>queue-number</i> [ <i>keyword</i> <i>key-value</i> ] | Establishes queueing priorities based on the protocol type.                                                                 |
| <b>queue-list</b> <i>list-number</i> <b>config-interface</b><br><i>interface-type</i> <i>interface-number</i> <i>queue-number</i>    | Establishes custom queueing based on packets entering from a given interface.                                               |
| <b>queue-list</b> <i>list-number</i> <b>default</b> <i>queue-number</i>                                                              | Assigns a queue number for those packets that do not match any other rule in the custom queue list. The default value is 1. |

| Command                                                                                                | Purpose                                         |
|--------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| <b>queue-list</b> <i>list-number protocol protocol-type</i><br><i>queue-number [keyword key-value]</i> | Establish a customized queue by protocol models |

To establish a customized queue by the protocol models, you can input :queue-list in the global configuration directory

```
[DEFAULT@Router/config/]#queue-list
```

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> Queue list number

Please Input the code of command to be execute(0-0): **0**

Please input a digital number:**2**

Key Word:

Q(quit)

(00)interface Establish priorities for packets from a named interface

(01)protocol Establish priorities for packets of a protocol

(02)queue configure parameters for a particular queue

(03)default set custom queue for unspecified packets

Please Input the code of command to be execute(0-3): **1**

Input 1 and select the<protocol> option

Key Word:

Q(quit)

(00)ip internet protocol

(01)arp Address Resolution Protocol

(02)comp\_tcp Compressed Tcp

Please Input the code of command to be execute(0-2): **0**

Key Word:

Q(quit)

(00)<0-16> Queue number

Please Input the code of command to be execute(0-0): **0**

Please input a digital number:**2**

Key Word:

Q(quit)

(00)gt Classify packets greater than a specified length

(01)lt Classify packets less than a specified length

(02)fragments Prioritize fragmented IP packets

(03)list to specify an access list

(04)tcp Prioritize TCP packets 'to' or 'from' the specified port

(05)udp Prioritize UDP packets 'to' or 'from' the specified port

(06)<cr>

Please Input the code of command to be execute(0-6): **0**

You can select different keyword at different needs.

Key Word:

Q(quit)

(00)<0-65535> packet length(include MAC encapsulation)

Please Input the code of command to be execute(0-0): **0**

Please input a digital number:**20**

Note : Input the size of <0-65535> packet, here 20 is only for example

Will you execute it? (Y/N):y

| Command                                                                                     | Purpose                                                      |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <b>queue-list</b> <i>list-number interface interface-type interface-number queue-number</i> | Establish CQ by a input packet from some specified interface |

To establish a customed queue by the protocol medols, you can input :queue-list in the global configuration directory

[DEFAULT@router /config/]#**queue-list**

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> Queue list number

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**2**

**Note** : Input 1-16 queue numbers here, 2 is only for example

Key Word:

Q(quit)

(00)interface Establish priorities for packets from a named interface

(01)protocol Establish priorities for packets of a protocol

(02)queue configure parameters for a particular queue

(03)default set custom queue for unspecified packets

Please Input the code of command to be excute(0-3): **0**

Input 0 and select interface option

Key Word:

Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

Please Input the code of command to be excute(0-4): **0**

Please input a interface name:**f0/0**

Input the port number that you want to configure

Key Word:

Q(quit)

(00)<0-16> Queue number

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**2**

**Note**: Input 1-16 queue number here, 2 is only for example

Will you excute it? (Y/N):**y**

| Command                                                   | Purpose                                                                                            |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>queue-list</b> <i>list-number default queue-number</i> | To assign a queue number for those that don't meet any rule of the customed list, the default is 1 |

Input :queue-list in the global configuration directory

[DEFAULT@4\_2750 /config/]#**queue-list**

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> Queue list number

Please Input the code of command to be excute(0-0): **0**

```

Please input a digital number:2
Key Word:
Q(quit)
(00)interface Establish priorities for packets from a named interface
(01)protocol Establish priorities for packets of a protocol
(02)queue configure parameters for a particular queue
(03)default set custom queue for unspecified packets
Please Input the code of command to be excute(0-3): 3
    Input3 ,select default option
Key Word:
Q(quit)
(00)<0-16> Queue number
Please Input the code of command to be excute(0-0): 0
Please input a digital number:2
Will you excute it? (Y/N):y

```

**Example:**

The following example assigns traffic that matches IP access list aaa to queue number 1:

```
queue-list 1 protocol ip 1 list aaa
```

The following example assigns Telnet packets to queue number 2

```
queue-list 4 protocols ip 2 tcp telnet
```

The following example assigns UDP Domain Name Service (DNS) packets to queue number 3

```
queue-list 4 protocol ip 3 udp dns
```

The following example assigns packets with more than 1000 bytes, to queue number 6

```
queue-list 5 protocol ip 6 gt 1000
```

**7.2.1.5 Configure PQ**

If you want to configure PQ to an interface, you can use the command below in interface configuration mode after the interface specified:

| Command                                  | Purpose                                                                                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>priority-group</b> <i>list-number</i> | Applying PQ to the interface, list-number is the number of the adopted customized queue list. The list argument is any number from 1 to 16. There is no default assignment. |

If you want to configure PQ on an interface, you can select **priority-group** in the interface commands under the global configuration directory after specifying the interface.

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> priority list number

Please Input the code of command to be excute(0-0):0

Input 0 and select <1-16>option, input the list number at prompt:

Please input a digital number:2

**Note :** Input 1-16 list numbers here, 2 is only for example.

Will you excute it? (Y/N):y

**Configuring Priority Queueing List**

The customized queueing can define the priority queueing lists, and specify the maximum number of the queues. When applying the list to an interface, you can adjust the parameters according to the list.

To specify the maximum number of the queues, use one of the following commands in global configuration mode:

| Command                                                                                                                       | Purpose                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>priority-list</b> <i>list-number</i> <b>queue-limit</b><br><i>high-limit middle-limit normal-limit</i><br><i>low-limit</i> | Specifies the maximum number of packets allowed in each of the priority queues. <i>high-limit 20, medium-limit 40, normal-limit 60, low-limit 80</i> |

To configure an upper limit for a PQ list, you can use this command in the global configuration directory:

```
[DEFAULT@Router /config/]#priority-list
```

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> priority list number

Please Input the code of command to be excute(0-0): **0**

Input 0, select <1-16>option and input the PQ list number at prompt:

Please input a digital number:**1**

**Note** : Input 1-16 PQ numers here, 1 is only for example.

Key Word:

Q(quit)

(00)interface Establish priorities for packets from a named interface

(01)protocol Establish priorities for packets of a protocol

(02)queue-limit set queue limit for priority queue

(03)default set custom queue for unspecified packets

Please Input the code of command to be excute(0-3): **2**

Input 2 and select<queue-limit> option:

Key Word:

Q(quit)

(00)<0-32767> High limit

Please Input the code of command to be excute(0-0): **0**

Input 0 and select <0-32767>option:

Please input a digital number:**15**

**Note** : Input the upper limit of 0 - 32767queue, 15 is only for example.

Key Word:

Q(quit)

(00)<0-32767> Middle limit

Please Input the code of command to be excute(0-0): **0**

Input 0 and select <0-32767>option:

Please input a digital number:**50**

**Note** : Input the middle value of 0 - 32767queue here, 50 is only for example.

Key Word:

Q(quit)

(00)<0-32767> Normal limit

Please Input the code of command to be excute(0-0): **0**

Input 0 and select <0-32767>option:

Please input a digital number:**70**

**Note** : Input a common value of 0 - 32767queue here, 70 is only for example.

Key Word:

Q(quit)

(00)<0-32767> Low limit

Please Input the code of command to be excute(0-0): **0**

Input 0 , select <0-32767> option :

Please input a digital number:100

**Note** : Input a lower value of the upper limit of 0 - 32767queue, 100 is only for example.

Will you excute it? (Y/N):y

**Example:**

Specifies the maximum number of packets allowed in each of the priority queues 10 50 70 100

priority-list 4 queue-limit 15 50 70 100

To specify which queue to place a packet in, use the following commands in global configuration mode:

| Command                                                                                                                                                                    | Purpose                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>priority-list</b> <i>list-number</i> <b>protocol</b> protocol-type { <b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b> } [ <i>keyword</i> <i>key-value</i> ]     | Establishes queueing priorities based on the protocol type.                                                                    |
| <b>priority-list</b> <i>list-number</i> <b>config-interface</b> <i>interface-type</i> <i>interface-number</i> { <b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b> } | Establishes queueing priorities for packets entering from a given interface.                                                   |
| <b>priority-list</b> <i>list-number</i> <b>default</b> <i>queue-number</i>                                                                                                 | Assigns a priority queue for those packets that do not match any other rule in the priority list, the default value is normal. |

| Command                                                                                                                                                                | Purpose                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <b>priority-list</b> <i>list-number</i> <b>protocol</b> protocol-type { <b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b> } [ <i>keyword</i> <i>key-value</i> ] | Establish PQ by the protocol type |

To configure the classification of a PQ list by the protocol type, you can input: priority-list:in a global configuration directory:

```
[DEFAULT@Router /config/]#priority-list
```

Key Word:

U(undo) D(default) Q(quit)

(00)<1-16> priority list number

Please Input the code of command to be excute(0-0): 0

Input 0, select <1-16>option, it will prompt to input the PQ number.

Please input a digital number:1

**Note** : Input numbers of 1-16 PQ list, 1 is only for example.

Key Word:

Q(quit)

(00)interface Establish priorities for packets from a named interface

(01)protocol Establish priorities for packets of a protocol

(02)queue-limit set queue limit for priority queue

(03)default set custom queue for unspecified packets

Please Input the code of command to be excute(0-3): 1

Input 1, select <protocol> option:

Key Word:

Q(quit)

(00)ip internet protocol

(01)arp Address Resolution Protocol

(02)comp\_tcp Compressed Tcp

Please Input the code of command to be excute(0-2): 0

**Note** : Input the protocol types here, 0 is only for example.

Key Word:

- Q(quit)
- (00)high
- (01)middle
- (02)normal
- (03)low

Please Input the code of command to be excute(0-3): 1

**Note** : Input PQ here, 1 is only for example.

Key Word:

- Q(quit)
- (00)gt           Classify packets greater than a specified length
- (01)lt           Classify packets less than a specified length
- (02)fragments   Prioritize fragmented IP packets
- (03)list         to specify an access list
- (04)tcp         Prioritize TCP packets 'to' or 'from' the specified port
- (05)udp         Prioritize UDP packets 'to' or 'from' the specified port
- (06)<cr>

Please Input the code of command to be excute(0-6): 0

**Note** : Input the keyword types here, 0 is only for example.

Key Word:

- Q(quit)
- (00)<0-65535> packet length(include MAC encapsulation)

Please Input the code of command to be excute(0-0): 0

Input 0 , select <0-65535> option :

Please input a digital number:34

**Note** : Input values of the 0 - 65535 keywords here, 34 is only for example.

Will you excute it? (Y/N):y

| Command                                                                                                                                                                | Purpose                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| <b>priority-list</b> <i>list-number</i> <b>interface</b> <i>interface-type</i><br><i>interface-number</i> { <b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b> } | Establish a PQ for the packets of some specified interface |

To configure the classification model of a PQ list by the interface models, you can input:priority-list in the global configuration directory.

[DEFAULT@Router /config/#]priority-list

Key Word:

- U(undo) D(default) Q(quit)
- (00)<1-16> priority list number

Please Input the code of command to be excute(0-0): 0

Input 0, select <1-16>option, it will prompt to input the PQ number.

Please input a digital number:1

Note: Input 1-16 priority list number, 1 is only for example.

Key Word:

- Q(quit)
- (00)interface    Establish priorities for packets from a named interface
- (01)protocol     Establish priorities for packets of a protocol
- (02)queue-limit  set queue limit for priority queue
- (03)default     set custom queue for unspecified packets

Please Input the code of command to be excute(0-3): 0

Input 0, select <interface>option :

Key Word:

Q(quit)  
 (00)FastEthernet FastEthernet interface  
 (01)Ethernet Ethernet interface  
 (02)Serial Serial interface  
 (03)Async Asynchronous interface

Please Input the code of command to be excute(0-3): 1

**Note** : Input the interface models here, 1 is only for example.

Please input a interface name:f0/0

**Note** : Input the interface name here, f0/0 is only for example.

Key Word:

Q(quit)  
 (00)high  
 (01)middle  
 (02)normal  
 (03)low

Please Input the code of command to be excute(0-3): 1

**Note** : Input the priority of the queue here, 1 is only for example.

Key Word:

Q(quit)  
 (00)<cr>

Please Input the code of command to be excute(0-0): 0

Will you excute it? (Y/N):y

Input y

| Command                                        | Purpose                                                                                               |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| priority-list list-number default queue-number | To assign a PQ for those packets that don't meet any rule of the priority list, the default is normal |

To configure a classification model for those packets that don ' t meet any rule, you can input:priority-list in the global cofiguration directory.

[DEFAULT@Router /config/]#priority-list

Key Word:

U(undo) D(default) Q(quit)  
 (00)<1-16> priority list number

Please Input the code of command to be excute(0-0): 0

Input0 ,select<1-16>option , it will prompt to input the PQ number :

Please input a digital number:1

**Note** : Input 1-16 priority list number of 1-16, 1 is only for example.

Key Word:

Q(quit)  
 (00)interface Establish priorities for packets from a named interface  
 (01)protocol Establish priorities for packets of a protocol  
 (02)queue-limit set queue limit for priority queue  
 (03)default set custom queue for unspecified packets

Please Input the code of command to be excute(0-3): 3

Input 3 ,select <default> option:

Key Word:

Q(quit)

- (00)high
- (01)middle
- (02)normal
- (03)low

Please Input the code of command to be excute(0-3): 1

**Note** : Input priority level of the queue, 1 is here only for example.

Will you excute it? (Y/N):y

## 7.2.2 QoS Display

### 7.2.2.1 Display The Interface Queues Information

In command to display the information of the interface queues, you can use the command below:

| Command                                                  | Purpose                                             |
|----------------------------------------------------------|-----------------------------------------------------|
| <b>show queue</b> <i>interface-type interface-number</i> | Displaying the information of the interface queues. |

[DEFAULT@Router /config/]#**show**

Key Word:

- U(undo) D(default) Q(quit)
- (00)alias alias for command
- (01)arp ARP table
- (02)backup Bakup status
- (03)board-info Board information
- (04)break router breakpoint information
- (05)
- (06)class-map show class-map configuration
- (07)configuration show configuration in flash memory
- (08)controller Interface controller status
- (09)cpu cpu usage information
- (10)debug State of each debugging option
- (11)dhcp DHCP information
- (12)dialer Dialer parameters and statistics
- (13)frame-relay Display Frame Relay state
- (14)frswitch Display Frame Relay switch state
- (15)hdlc HDLC parameters and statistics
- (16)hosts Host table
- (17)interface interface status and configuration
- (18)ip IP information
- (19)job Job parameters and statistics
- (20)l2tp L2TP information
- (21)line TTY line information
- (22)llc LLC2 parameters and statistics
- (23)logging Show the contents of logging buffers
- (24)memory memory info
- (25)pdp pdp State information
- (26)policy-map show policy-map configuration
- (27)ppp PPP parameters and statistics

```
(28)queue show queue contents
--More--
```

**28**

Input 28, select queueoption.

Key Word:

```
Q(quit)
(00)FastEthernet   FastEthernet interface
(01)Ethernet       Ethernet interface
(02)Serial          Serial interface
(03)Async           Asynchronous interface
```

Please Input the code of command to be excute(0-3): **1**

Note : Input interface type here, 1 is only for example.

Please input a interface name:**f0/0**

Note : Input interface name here, f0/0is only for example.

Will you excute it? (Y/N):y

The screen will display the queue information like the following:

```
priority-list 2
```

```
Output queues: (queue :size/max/drops):
```

```
high: 0/50/0 middle: 0/24/0 normal: 0/1/0 low: 0/1/0
```

### 7.2.2.2 Display The Customed List Configuration

In command to display the customed queueing configuration, you can use the command below:

| Command                     | Purpose                                         |
|-----------------------------|-------------------------------------------------|
| <b>show queueing custom</b> | Displaying the customed queueing configuration. |

```
[DEFAULT@Router /config/]#show
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)alias    alias for command
(01)arp      ARP table
(02)backup   Bakup status
(03)board-info Board information
(04)break router breakpoint information
(05)
(06)class-map show class-map configuration
(07)configuration show configuration in flash memory
(08)controller Interface controller status
(09)cpu cpu usage information
(10)debug State of each debugging option
(11)dhcp DHCP information
(12)dialer Dialer parameters and statistics
(13)frame-relay Display Frame Relay state
(14)frswitch Display Frame Relay switch state
(15)hdlc HDLC parameters and statistics
(16)hosts Host table
(17)interface interface status and configuration
(18)ip IP information
(19)job Job parameters and statistics
```

- (20)l2tp L2TP information
- (21)line TTY line information
- (22)llc LLC2 parameters and statistics
- (23)logging Show the contents of logging buffers
- (24)memory memory info
- (25)pdp pdp State information
- (26)policy-map show policy-map configuration
- (27)ppp PPP parameters and statistics
- (28)queue show queue contents
- More--

**28**

Input 28 , select queue option

Key Word:

Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

Please Input the code of command to be excute(0-3): **1**

Note : Input interface info here, **1** is only for example

Please input a interface name:**f0/0**

Note : Input interface info here, **f0/0**is only for example

Will you excute it? (Y/N):y

The screen will display :

priority-list 2

Output queues: (queue :size/max/drops):

high: 0/50/0 middle: 0/24/0 normal: 0/1/0 low: 0/1/0

### 7.2.2.3 Display the priority list configuration

In command to display the priority queueing configuration, you can use the command below:

| Command                       | Purpose                                      |
|-------------------------------|----------------------------------------------|
| <b>show queueing priority</b> | Display the priority queueing configuration. |

[DEFAULT@Router /config/]#**show**

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command

(01)arp ARP table

(02)backup Bakup status

(03)board-info Board information

(04)break router breakpoint information

(05)

(06)class-map show class-map configuration

(07)configuration show configuration in flash memory

(08)controller Interface controller status

(09)cpu cpu usage information

(10)debug State of each debugging option

(11)dhcp DHCP information

(12)dialer Dialer parameters and statistics

- (13)frame-relay Display Frame Relay state
- (14)frswitch Display Frame Relay switch state
- (15)hdlc HDLC parameters and statistics
- (16)hosts Host table
- (17)interface interface status and configuration
- (18)ip IP information
- (19)job Job parameters and statistics
- (20)l2tp L2TP information
- (21)line TTY line information
- (22)llc LLC2 parameters and statistics
- (23)logging Show the contents of logging buffers
- (24)memory memory info
- (25)pdp pdp State information
- (26)policy-map show policy-map configuration
- (27)ppp PPP parameters and statistics
- (28)queue show queue contents
- (29)queueing show queueing configuration

--More--

## 29

Input 29 , select queueing option

Key Word:

Q(quit)

(00)custom custom queue list configuration

(01)priority priority queue list configuration

Please Input the code of command to be excute(0-1):0

Input 0 , select <custom> option :

Will you excute it? (Y/N):y

The screen will display configuration like the following lines:

Current custom queue list configuration :

List Queue Args

### 7.2.2.4 Display the class-map configuration

In command to display the class-map configuration, you can use the command below:

| Command                                            | Purpose                             |
|----------------------------------------------------|-------------------------------------|
| <b>show config-class-map</b> [ <i>class-name</i> ] | Display the class-map configuration |

[DEFAULT@Router /config/]#show

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command

(01)arp ARP table

(02)backup Bakup status

(03)board-info Board information

(04)break router breakpoint information

(05)

(06)class-map show class-map configuration

--More--

## 6

Input 6 , select class-map option

Key Word:

Q(quit)

(00)WORD class-map name

<cr>

Please Input the code of command to be excute(0-0): 0

Input 0 , select WORD option :

Please input a string:**name**

Note: Input class map names here, name is only for example.

Will you excute it? (Y/N):y

The screen will display the configuration like the following lines:

Class-Map name

match access-group name

### 7.2.2.5 Display The Policy-map Configuration

In command to display the policy-map configuration, you can use the command below:

| Command                                       | Purpose                               |
|-----------------------------------------------|---------------------------------------|
| <b>show policy-map</b> [ <i>policy-name</i> ] | Display the policy-map configuration. |

To display your policy map configuration, you can use: show policy-map command in the global configuration directory.

[DEFAULT@Router /config/]#**show**

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command

(01)arp ARP table

(02)backup Backup status

(03)board-info Board information

(04)break router breakpoint information

(05)

(06)class-map show class-map configuration

(07)configuration show configuration in flash memory

(08)controller Interface controller status

(09)cpu cpu usage information

(10)debug State of each debugging option

(11)dhcp DHCP information

(12)dialer Dialer parameters and statistics

(13)frame-relay Display Frame Relay state

(14)frswitch Display Frame Relay switch state

(15)hdlc HDLC parameters and statistics

(16)hosts Host table

(17)interface interface status and configuration

(18)ip IP information

(19)job Job parameters and statistics

(20)l2tp L2TP information

(21)line TTY line information

(22)llc LLC2 parameters and statistics

(23)logging Show the contents of logging buffers

(24)memory memory info

```
(25)pdp      pdp State information
(26)policy-map show policy-map configuration
```

```
--More--
```

## 26

Input 26 , select policy-map option

Key Word:

Q(quit)

(00)WORD policy-map name

Please Input the code of command to be excute(0-0):0

Input 0 , select WORD option :

Please input a string:name

Note : Input policy map names here, name is only for example.

Will you excute it? (Y/N):y

The screen displays the policy map configuration like the following lines:

```
Policy-Map name
```

### 7.2.3 QoS Configuration Project

If you have four types application A, B, C and D, the desired bandwidth ratio is 10:20:40:30, the packet size is 1428:582:371:1525. When the system serves a queue, it will send integral times bytes of the packet size, so you must take the packet size into account when you configure the total bytes, not specify them into 100:200:400:300 simply, in this way, the bandwidth ratio must be 1428:582:371:1525. In command to achieve the purpose, follow these steps:

Step 1: Produce a ratio of all frame sizes, dividing the percentages of bandwidth you want each queue to have into its frame size. The ratios would be: 10/1428,20/582,40/371,30/1525 or 0.007,0.03436,0.10782,0.01967.

Step 2: Normalize the ratios by the smallest value, that is: 1,4.9,15.4,2.8, This is the ratio of the number of frames that must be sent.

Spet 3: Note that any fraction in any of the ratio values means that an additional frame will be sent. The integer part of the ratio is the total number of frames that must be sent. In the example above, the ratio of the number of frames that must be sent would be 1:5:16: 3.

Step 4: Now multiply the results by the percentages of bandwidth you want each protocol to have, in this way, you can convert the ratio of the number of frames into bytes quantity. In this example, the router would send one 1428-byte frame, five 582-byte frames, sixteen 371-byte frames and three 1525-byte frames. That is, every queue sends 1428, 2910, 5936, and 4575 bytes. It is the bytes quantity you will specify in the customized queueing configuration.

Step 5: To determine the bandwidth distribution this represents, first determine the total number of bytes sent after all four queues are serviced:  $(1 \times 1428) + (5 \times 582) + (16 \times 371) + (3 \times 1525) = 1428 + 2910 + 5936 + 4575 = 14849$ . Then determine the percentage of the 14849 bytes that was sent from each queue:  $1428/14849, 2910/14849, 5936/14849, 4575/14849 = 9.6\%, 19.5\%, 39.8\%$  and  $30.8\%$ . As you can see, this is close to the desired ratio of 10:20:40:30.

Step 6: The resulting bandwidth allocation can be tailored further by multiplying the original ratio by an appropriate value, and trying to get as close to four integer values as possible. Note: The multiplier needn't be an integer.

The detail configuration is showed below: (Supposed the four applications are udp port 100, 200, 400, 700 respectively; and use the NO. 1 custom queue list).

First assign appropriate queue (2, 3, 4, 5) to the four applications:

```
queue-list 1 p ip 2 udp 100
queue-list 1 p ip 3 udp 200
queue-list 1 p ip 4 udp 400
```

```
queue-list 1 p ip 5 udp 700
```

Specify the total bytes that must be sent for every queue

```
queue-list 1 queue 2 byte-count 1428
```

```
queue-list 1 queue 3 byte-count 2910
```

```
queue-list 1 queue 4 byte-count 5936
```

```
queue-list 1 queue 5 byte-count 4575
```

Configure the custom queue list to the interface

```
interface s0/0
```

```
custom-queue-list 1
```

### 7.3 Configure RTP Header Compression Protocol

This chapter describes how to configure Compressed Real-Time Protocol (CRTP) header on serial lines using. To locate documentation of commands that appear in this chapter, see the “[RTP Header Compression Command](#)”.

#### 7.3.1 CRT Configuration Steps

To configure CRTP header, perform the tasks in the following sections.

[Enable CRTP on a Serial Interface](#)

[Change the Maximum Number of CRTP Connections](#)

[Display CRTP Compression Information](#)

[CRTP Debugging](#)

Note: You must enable CRTP on both ends of a serial connection, otherwise, it’s unavailable.

#### 7.3.2 Brief Introduction Of CRTP

The Router CRTP is only supported on serial lines using PPP encapsulation currently, and we will support on Frame Relay, HDLC encapsulation and over ISDN interfaces in the future.

You should configure CRTP if the following conditions exist in your network:

- Slow links
- The need to save bandwidth

CRTP is a very effective way to the above situations, you can see the advantage from the figure below:



In the best condition, the IP header without options is 20 bytes and the minimum size of the RTP header is 12 bytes, adding 8 bytes of the UDP header, the total bytes of these headers is 40 bytes; when sends the RTP payload with two

frames every time in G.729 call, then the payload is 20 bytes; adding 4 bytes PPP link layer encapsulation, the payload ratio is only 31.25 percents.

Using RTP Header-Compression (cRTP) and ignoring the UDP check sum these headers can be compressed to 2 bytes, adding 4 bytes PPP link layer encapsulation, the payload ratio is 76.92 percents, there is a very big gap between them.

**Note:** CRTP should not be used on links greater than 2 Mbps.

### 7.3.3 Enable CRTP On A Serial Interface

To enable CRTP header for serial encapsulations PPP, use the following command in interface configuration mode: (You must enable compression on both ends of a serial connection.)

| Command                                                             | Description |
|---------------------------------------------------------------------|-------------|
| ip rtp header-compression [{ cisco-format   iphc-format   passive}] | Enable CRTP |

The optional parameter *cisco-format*, which specifies IPCP to adopt packets with D-Link format when CRTP is applied to PPP links, is a default value; If you include the **passive** keyword which specifies IPCP to adopt packets with D-Link format when CRTP is applied to PPP links, the software compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed; the key word *iphc-format* specifies IPCP to adopt packets with RFC2509 format when CRTP is applied to PPP links

```
[DEFAULT@Router /config/#]interface
```

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

(08)Multilink Multilink-group interface

(09)Virtual-template Virtual template interface

(10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): 2

Input 2 , select Serial

Please input a interface name:s2/0

Note : Enter a serial interface environment, s2/0 is only for example.

Will you excute it? (Y/N):y

Key Word:

Q(quit)

(00)arp set arp timeout

(01)backup Modify backup parameters

(02)bandwidth Set the interface bandwidth

(03)bridge-group Transparent bridging interface parameters

(05)chinese help message in Chinese

(06)chmem Change memory of system

(07)clear\_drv clear interface statistic counter

```

(08)crypto Encryption module
(09)custom-queue-list Assign a custom queue list to interface
(10)default restore default configuration
(11)delay Set the interface delay
(12)description Set the interface description
(13)duplex Configure duplex operational mode
(14)english help message in English
(15)exit exit / quit
(16)fair-queue enable fair queue on interface
(17)help Description of the interactive help system
(18)history look up history
(19)interface interface configuration
(20)ip IP configuration commands
(21)keepalive Enable keepalive
(22)llc2 Setup LLC2(Logic Link Control Type2) parameters
(23)no negate configuration
(24)pdp pdp configuration commands
(25)physical-interface Configure lan physical interface
(26)pppoe-client pppoe client enable
(27)priority-group Assign a priority group to interface
(29)random-detect enable weighted random early detect on interfac
e
(30)router routing protocol configuration
(31)service-policy Assign a priority group to interface
(32)show show configuration and status
(33)shutdown Shutdown the current interface
(34)snmp Modify SNMP interface parameters
(35)speed Configure speed operation
Please Input the code of command to be excute(0-35): 20 (select ip)
Will you excute it? (Y/N):y
Key Word:
U(undo) D(default) Q(quit)
(00)access-group Specify access control for packets
(01)address IP address
(02)beigrp Enhanced Interior Gateway Routing Protocol
(03)directed-broadcast Enable forwarding of directed broadcasts
(04)fast-switch Fast-Switch interface commands
(05)helper-address Specify a destination address for UDP broadcasts
(06)irdp ICMP Router Discovery Protocol
(07)mask-reply Enable sending ICMP Mask Reply messages
(08)mtu Maximum Transmission Unit
(09)nat NAT interface commands
(10)ospf set OSPF parameter for this port
(11)redirects Enable sending ICMP Redirect messages
(12)rip set RIP parameter for this port
(13)route-cache Enable fast-switching cache for outgoing packets
(14)rsvp RSVP interface command
(15)rtp Rtp parameters
(16)tcp Tcp parameters

```

(17)unnumbered Enable IP processing without an explicit address

(18)unreachables Enable sending ICMP Unreachable messages

Please Input the code of command to be excute(0-18): 15

Input 15 ,select rtp:

Key Word:

Q(quit)

(00)compression-connections Maximum number of compressed connections

(01)header-compression Enable RTP header compression

Please Input the code of command to be excute(0-1): 1

Input 1 ,select header-compression:

Key Word:

U(undo) D(default) Q(quit)

(00)iphc-format Use RFC 2509 format IPCP

(01)cisco-format Use Cisco format IPCP

(02)passive Compress only for destinations which send compressed headers

(03)<cr>

Please Input the code of command to be excute(0-3): 1

Input 1 ,select <cisco-format> option :

Will you excute it? (Y/N):y

### 7.3.4 Change The Maximum Number Of CRTP Connections

| Command                                      | Description                                           |
|----------------------------------------------|-------------------------------------------------------|
| ip rtp compression-connections <i>number</i> | Specify the maxumun number of local CRTP connections. |

CRTP will locally keep the structure storage connecting information for each specified transmitting address. If the specified connecting number is not enough, these structures can not provide correspondence for simultaneously running multi-RTP conversations and affect the quality of compression.

Select ip command under the configure interface directory

Key Word:

U(undo) D(default) Q(quit)

(00)access-group Specify access control for packets

(01)address IP address

(02)beigrp Enhanced Interior Gateway Routing Protocol

(03)directed-broadcast Enable forwarding of directed broadcasts

(04)fast-switch Fast-Switch interface commands

(05)helper-address Specify a destination address for UDP broadcasts

(06)irdp ICMP Router Discovery Protocol

(07)mask-reply Enable sending ICMP Mask Reply messages

(08)mtu Maximum Transmission Unit

(09)nat NAT interface commands

(10)ospf set OSPF parameter for this port

(11)redirects Enable sending ICMP Redirect messages

(12)rip set RIP parameter for this port

(13)route-cache Enable fast-switching cache for outgoing packets

(14)rsvp RSVP interface command

(15)rtp Rtp parameters

(16)tcp Tcp parameters

(17)unnumbered Enable IP processing without an explicit address

(18)unreachables Enable sending ICMP Unreachable messages

Please Input the code of command to be excute(0-18): 15

Input 15 , select rtp:

Key Word:

Q(quit)

(00)compression-connections Maximum number of compressed connections

(01)header-compression Enable RTP header compression

Please Input the code of command to be excute(0-1):0

Input 0 , select compression-connections

Key Word:

Q(quit)

(00)<3-256> Number of connections

Please Input the code of command to be excute(0-0): 0

Input 0, select <3-256>option, it will prompt to input the max connection number:

Please input a digital number:Please input a string:45

Note : Input the max connection number of CRTP here, 45 is only for example.

Will you excute it? (Y/N):y

#### 7.3.4 Display CRTP Compression Information

| Command                                                                        | Description                          |
|--------------------------------------------------------------------------------|--------------------------------------|
| <b>show ip rtp header-compression</b> [ <i>type number</i> ] [ <b>detail</b> ] | display CRTP compression imformation |

The above commands need to be configured under the global configuration directory.

[DEFAULT@Router /enable/#]show

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command

(01)arp ARP table

(02)backup Bakup status

(03)board-info Board information

(04)break router breakpoint information

(05)

(06)class-map show class-map configuration

(07)configuration show configuration in flash memory

(08)controller Interface controller status

(09)cpu cpu usage information

(10)debug State of each debugging option

(11)dhcp DHCP information

(12)dialer Dialer parameters and statistics

(13)frame-relay Display Frame Relay state

(14)frswitch Display Frame Relay switch state

(15)hdlc HDLC parameters and statistics

(16)hosts Host table

(17)interface interface status and configuration

(18)ip IP information

(19)job Job parameters and statistics

(20)l2tp L2TP information

--More--

18

Input 18 , select ip option :

Key Word:

Q(quit)

(00)access-lists List IP access lists  
 (01)as-path-list Information of AS-Path list  
 (02)beigrp Show BEIGRP information  
 (03)bgp BGP information  
 (04)cache IP route cache  
 (05)community-list Information of community-list  
 (06)dhcpd DHCP Server information  
 (07)fast-switch Fast-switch information  
 (08)interface IP interface status and configuration  
 (09)irdp ICMP Router Discovery Protocol  
 (10)local Specify local options  
 (11)nat IP NAT information  
 (12)ospf show OSPF information  
 (13)prefix-list Prefix-list definition  
 (14)rip Routing Information Protocol(RIP)  
 (15)route show route table  
 (16)rsvp - rsvp information  
 (17)rtp Rtp parameters  
 (18)sockets Open IP sockets  
 (19)tcp Tcp parameters  
 (20)traffic Traffic statistics

--More--

17

Input 17 , select rtp option :

Key Word:

Q(quit)

(00)header-compression RTP/UDP/IP header-compression statistics

Please Input the code of command to be excute(0-0): 0

Input 0 , select header-compression option

Key Word:

Q(quit)

(00)Serial Serial interface

(01)Async Asynchronous interface

Please Input the code of command to be excute(0-1): Key Word:

Q(quit)

(00)<cr>

Please Input the code of command to be excute(0-0): 0

Input 0 , <cr>:

Will you excute it? (Y/N):y

The Screen will display CRTP information like the following:

RTP/UDP/IP header compression statistics:

Interface Serial2/0:

You must use the command in global configuraion mode.

### 7.3.5 CRTP Debugging

| Command | Description |
|---------|-------------|
|---------|-------------|

|                                               |                                                                                   |
|-----------------------------------------------|-----------------------------------------------------------------------------------|
| <b>debug config-ip rtp header-compression</b> | display the information of the received and transformed CRTP packets information. |
|-----------------------------------------------|-----------------------------------------------------------------------------------|

The above commands should be used under the global configuration directory.

```
[DEFAULT@Router /enable/]#debug
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)aaa Debug AAA process information
(01)arp IP ARP transactions
(02)backup debug backup information
(03)chat Chat scripts activity
(04)custom-queue debug custom output queue
(05)dhcp DHCP client activity
(06)dialer Dial on Demand event
(07)frame-relay Debug Frame Relay information
(08)gpl gpl transmit and receive
(09)gre Generic routing encapsulation
(10)hdlc HDLC information
(11)interface Interface transmit and receive
(12)ip IP information
(13)job Debug job information
(14)l2tp L2TP information
(15)lapb LAPB information
(16)line recv and send data on line
(17)llc2 Debug LLC2 information
(18)ppp debug PPP information
(19)pppoe Debug pppoe information
(20)priority debug priority output queue
```

```
--More--
```

```
12
```

```
Input 12 , select ip option
```

Key Word:

```
Q(quit)
(00)beigrp Trace BEIGRP information
(01)bgp trace BGP information
(02)dhcpcd DHCP Server activity
(03)icmp ICMP transactions
(04)nat NAT debug commands
(05)ospf trace OSPF information
(06)packet IP packet processing
(07)raw Raw IP packet received and sent
(08)rip trace RIP information
(09)rsvp RSVP packet processing
(10)rtp Rtp parameters
(11)tcp TCP information
(12)udp UDP transactions
```

Please Input the code of command to be excute(0-12): 10

```
Input 10, select rtp option
```

Key Word:

```
Q(quit)
```

```
(00)header-compression RTP header compression
(01)packets RTP packets
(02)rtcp RTCP packets
Please Input the code of command to be excute(0-2): 0
Input 0, select header-compression option
Will you excute it? (Y/N):y
The screen will display the CRTP information like the following:
RTP header compression debug is enalbed!
```

You must use the command in global configuraion mode.

### 7.3.6 Configuration Examples

The following example shows how to configure the CRTP on serial lines using Point-to-Point Protocol (PPP) encapsulation:

```
interface serial 1/2
ip rtp header-compression
ip rtp compression-connections 25
encapsulation ppp
7.4 Configure CTCP (TCP/ IP Header-Compression Protocol)
```

This section briefly describes how to configure TCP/IP header-compression protocol on serial link using PPP. Please refer to the command description of TCP/IP header-compression for details.

#### 7.4.1 CTCP Configuration Steps

There are a few steps to configure CTCP:

```
Enable CTCP On A Serial Interface
Change The Maximum Number Of CTCP Connections
Display CTCP Compression Information
CTCPDebugging
```

**Note: You must configure CTCP on both ends of a serial connection, otherwise the CTCP is unavailable.**

#### 7.4.2 About CTCP

Currently the CTCP can only support the serial link encapsulated as PPP, and it can expand to Frame Relay, HDLC encapsulation and ISDN interface. We need to configure CTCP in these cases:

- Slow serial links
- The serial links need to save bandwidth

Supposing operating on a communication link that need abundant TELNET, each time of click from client end need to be loaded by a TCP message, and if the size of IP, TCP header without options are totally 40 bytes but payload is only 1 byte, so the efficiency is quite lower.

If you choose to carry the same message with CTCP, you need only 4 byte header (TCP/IP head-compression standard stimulated by rfc2507), or 3 bytes (TCP/IP head-compression standard stimulated by rfc1144).

**Note** CRTP should not be used on links greater than 2 Mbps.

### 7.4.3 Enable CTCP On A Serial Line

To enable CTCP header for serial encapsulations PPP, use the following command in interface configuration mode: (You must enable compression on both ends of a serial connection.)

| Command                                                             | Description |
|---------------------------------------------------------------------|-------------|
| ip tcp header-compression [{ cisco-format   iphc-format   passive}] | Enable CTCP |

The optional parameter *cisco-format* is a default value, which specifies IPCP to adopt packets with cisco format when the IPHC format CRTP is applied to PPP links, else the IPCP packet format is RFC1144; If you include the **passive** keyword, the software compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed, when the CRTP is applied to PPP links, IPCP will adopt the cisco format packet if CRTP is IPHC format, else the IPCP will adopt RFC1144 format packet; the key word *iphc-format* specifies IPCP to adopt packets with RFC2509 format when CRTP is applied to PPP links. However, if the opposite terminal PPP implementation support only CTCP of RFC1144, IPCP of RFC1144 can be used in the same. But if you apply CTCP on FR and HDLC link, cisco-format will adopt CTCP of RFC1144, iphc-format will adopt CTCP of RFC2507, and passive show our CTCP is determined by CTCP message format that sent by opposite terminal.

Input the following commands under the interface-serial of global configuration directory:

```
[DEFAULT@Router /config/#]interface
```

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

(08)Multilink Multilink-group interface

(09)Virtual-template Virtual template interface

(10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): 2

Input 2 ,select Serial option

Please input a interface name:s2/0

Note : Input the interface name here ,s2/0 is only for example

Will you excute it? (Y/N):y

Key Word:

Q(quit)

(00)arp set arp timeout

(01)backup Modify backup parameters

(02)bandwidth Set the interface bandwidth

(03)bridge-group Transparent bridging interface parameters

(05)chinese help message in Chinese

(06)chmem Change memory of system

(07)clear\_drv clear interface statistic counter

(08)crypto Encryption module

(09)custom-queue-list Assign a custom queue list to interface

(10)default restore default configuration

(11)delay Set the interface delay

(12)description Set the interface description  
 (13)duplex Configure duplex operational mode  
 (14)english help message in English  
 (15)exit exit / quit  
 (16)fair-queue enable fair queue on interface  
 (17)help Description of the interactive help system  
 (18)history look up history  
 (19)interface interface configuration  
 (20)ip IP configuration commands  
 (21)keepalive Enable keepalive  
 (22)llc2 Setup LLC2(Logic Link Control Type2) parameters  
 (23)no negate configuration  
 (24)pdp pdp configuration commands  
 (25)physical-interface Configure lan physical interface  
 (26)ppoe-client pppoe client enable  
 (27)priority-group Assign a priority group to interface  
 (29)random-detect enable weighted random early detect on interface  
 e  
 (30)router routing protocol configuration  
 (31)service-policy Assign a priority group to interface  
 (32)show show configuration and status  
 (33)shutdown Shutdown the current interface  
 (34)snmp Modify SNMP interface parameters  
 (35)speed Configure speed operation  
 Please Input the code of command to be excute(0-35): 20 (option ip)  
 Will you excute it? (Y/N):y

## Key Word:

U(undo) D(default) Q(quit)  
 (00)access-group Specify access control for packets  
 (01)address IP address  
 (02)beigrp Enhanced Interior Gateway Routing Protocol  
 (03)directed-broadcast Enable forwarding of directed broadcasts  
 (04)fast-switch Fast-Switch interface commands  
 (05)helper-address Specify a destination address for UDP broadcasts  
 (06)irdp ICMP Router Discovery Protocol  
 (07)mask-reply Enable sending ICMP Mask Reply messages  
 (08)mtu Maximum Transmission Unit  
 (09)nat NAT interface commands  
 (10)ospf set OSPF parameter for this port  
 (11)redirects Enable sending ICMP Redirect messages  
 (12)rip set RIP parameter for this port  
 (13)route-cache Enable fast-switching cache for outgoing packets  
 (14)rsvp RSVP interface command  
 (15)rtp Rtp parameters  
 (16)tcp Tcp parameters  
 (17)unnumbered Enable IP processing without an explicit address  
 (18)unreachables Enable sending ICMP Unreachable messages  
 Please Input the code of command to be excute(0-18): 16

Input 16 , select tcp option

Key Word:

Q(quit)

(00)compression-connections Maximum number of compressed connections

(01)header-compression Enable TCP header compression

Please Input the code of command to be excute(0-1): 1

Input 1 , select header-compression option

Key Word:

Q(quit)

(00)iphc-format Use RFC 2509 format IPCP

(01)cisco-format Use Cisco format IPCP

(02)passive Compress only for destinations which send compressed headers

(03)<cr>

Please Input the code of command to be excute(0-3): 1

Note : Select corresponding parameters to meet clients ' need, 1 is only for example.

Will you excute it? (Y/N):y

#### 7.4.4 Change The Maximum Number Of CTCP Connections

| Command                                             | Description                                                                  |
|-----------------------------------------------------|------------------------------------------------------------------------------|
| <b>ip tcp compression-connections</b> <i>number</i> | Specify the maximum number of CTCP connections supported on local interface. |

CTCP will locally keep the structure storage connecting information for each specified transmitting address. If the specified connecting number is not enough, these structures can not provide correspondence for simultaneously running multi-TCP conversations and affect the quality of compression.

Select ip command under the configre interface directory:

Key Word:

U(undo) D(default) Q(quit)

(00)access-group Specify access control for packets

(01)address IP address

(02)beigrp Enhanced Interior Gateway Routing Protocol

(03)directed-broadcast Enable forwarding of directed broadcasts

(04)fast-switch Fast-Switch interface commands

(05)helper-address Specify a destination address for UDP broadcasts

(06)irdp ICMP Router Discovery Protocol

(07)mask-reply Enable sending ICMP Mask Reply messages

(08)mtu Maximum Transmission Unit

(09)nat NAT interface commands

(10)ospf set OSPF parameter for this port

(11)redirects Enable sending ICMP Redirect messages

(12)rip set RIP parameter for this port

(13)route-cache Enable fast-switching cache for outgoing packets

(14)rsvp RSVP interface command

(15)rtp Rtp parameters

(16)tcp Tcp parameters

(17)unnumbered Enable IP processing without an explicit address

```
(18)unreachables Enable sending ICMP Unreachable messages
Please Input the code of command to be excute(0-18): 16
Input 16 , select tcp option
Key Word:
Q(quit)
(00)compression-connections Maximum number of compressed connections
(01)header-compression Enable TCP header compression
Please Input the code of command to be excute(0-1): 0
Input 0 , select compression-connections option
Key Word:
  Q(quit)
  (00)<3-256> Number of connections
Please Input the code of command to be excute(0-0): 0
Input 0 , select <3-256> option :
Please input a digital number:Please input a string:4
Note : Input the max CTCP connection number of 3-256 here, 4 is only for example.
Will you excute it? (Y/N):y
```

#### 7.4.5 Display CTCP Compression Information

| Command                                                                        | Description               |
|--------------------------------------------------------------------------------|---------------------------|
| <b>show ip tcp header-compression</b> [ <i>type number</i> ] [ <i>detail</i> ] | Display CTCP information. |

The above commands need to be used under the global configuration directory.

```
[DEFAULT@Router /enable/]#show
Key Word:
U(undo) D(default) Q(quit)
(00)alias alias for command
(01)arp ARP table
(02)backup Backup status
(03)board-info Board information
(04)break router breakpoint information
(05)
(06)class-map show class-map configuration
(07)configuration show configuration in flash memory
(08)controller Interface controller status
(09)cpu cpu usage information
(10)debug State of each debugging option
(11)dhcp DHCP information
(12)dialer Dialer parameters and statistics
(13)frame-relay Display Frame Relay state
(14)frswitch Display Frame Relay switch state
(15)hdlc HDLC parameters and statistics
(16)hosts Host table
(17)interface interface status and configuration
(18)ip IP information
(19)job Job parameters and statistics
(20)l2tp L2TP information
--More
18
```

Input 18 , select ip option

Key Word:

Q(quit)

- (00)access-lists List IP access lists
- (01)as-path-list Information of AS-Path list
- (02)beigrp Show BEIGRP information
- (03)bgp BGP information
- (04)cache IP route cache
- (05)community-list Information of community-list
- (06)dhcpd DHCP Server information
- (07)fast-switch Fast-switch information
- (08)interface IP interface status and configuration
- (09)irdp ICMP Router Discovery Protocol
- (10)local Specify local options
- (11)nat IP NAT information
- (12)ospf show OSPF information
- (13)prefix-list Prefix-list definition
- (14)rip Routing Information Protocol(RIP)
- (15)route show route table
- (16)rsvp - rsvp information
- (17)rtp Rtp parameters
- (18)sockets Open IP sockets
- (19)tcp Tcp parameters
- (20)traffic Traffic statistics

--More--

19

Input 19 , select tcp option

Key Word:

Q(quit)

- (00)header-compression RTP/UDP/IP header-compression statistics

Please Input the code of command to be excute(0-0): 0

Input 0 , select header-compression option

Key Word:

Q(quit)

- (00)Serial Serial interface
- (01)Async Asynchronous interface

Please Input the code of command to be excute(0-1): Key Word:

Q(quit)

- (00)<cr>

Please Input the code of command to be excute(0-0): 0

Input 0 , select <cr> option :

Will you excute it? (Y/N):y

The secreen will display the CTCP information like the following:

IP/TCP header compression statistics:

Interface Serial2/0:

You must use the command in interface configuration mode.

## 7.4.6 CTCP Debugging

| Command                         | Description                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------|
| debug ip tcp header-compression | Display the information of the received and transformed CTCP packets information. |

The above commands need to be used under the global configuration directory:

```
[DEFAULT@Router /enable/]#debug
```

Key Word:

U(undo) D(default) Q(quit)

(00)aaa Debug AAA process information

(01)arp IP ARP transactions

(02)backup debug backup information

(03)chat Chat scripts activity

(04)custom-queue debug custom output queue

(05)dhcp DHCP client activity

(06)dialer Dial on Demand event

(07)frame-relay Debug Frame Relay information

(08)gpl gpl transmit and receive

(09)gre Generic routing encapsulation

(10)hdlc HDLC information

(11)interface Interface transmit and receive

(12)ip IP information

(13)job Debug job information

(14)l2tp L2TP information

(15)lapb LAPB information

(16)line recv and send data on line

(17)llc2 Debug LLC2 information

(18)ppp debug PPP information

(19)pppoe Debug pppoe information

(20)priority debug priority output queue

--More--

12

Input 12 , select ipoption

Key Word:

Q(quit)

(00)beigrp Trace BEIGRP information

(01)bgp trace BGP information

(02)dhcpcd DHCP Server activity

(03)icmp ICMP transactions

(04)nat NAT debug commands

(05)ospf trace OSPF information

(06)packet IP packet processing

(07)raw Raw IP packet received and sent

(08)rip trace RIP information

(09)rsvp RSVP packet processing

(10)rtp Rtp parameters

(11)tcp TCP information

(12)udp UDP transactions

Please Input the code of command to be excute(0-12): 11

Input 11 , select tcp option :

Key Word:

Q(quit)

(00)header-compression TCP header compression

(01)packet TCP packets

(02)transactions Significant TCP events

Please Input the code of command to be excute(0-2): 0

Input 0 , select header-compression option

Will you excute it? (Y/N):y

The screen will display the CTCP information like the following:

TCP header compression debug is enalbed!

You must use the command in interface configuration mode.

#### 7.4.7 Configuration Example

The following example shows how to configure the CTCP on serial lines using Point-to-Point Protocol (PPP) encapsulation:

```
interface serial 1/2
```

```
ip tcp header-compression
```

```
ip tcp compression-connections 25
```

```
encapsulation ppp
```

### 8. Dialer Configuration

#### 8.1 About dialer

D-Link router provides perfect dialer solution for user:

- Support dialer interface backup, meet all kinds of backup requirements
- Support all kinds of dialer interfaces, such as asynchronous or synchronous serial interface.
- Provide DDR dialer function to meet the requirement of user.
- Dialer link layer supports PPP and SLIP network layer protocol.
- Support route protocols (such as RIP1/RIP2 or OSPF) running on the dialer interface

#### 8.2 Software Configuration of Dialer

This section describes how to configure dialer on router. Please refer to the [“Dialer Configuration Command”](#) for related configuration command.

#### 8.3 Dialer Configuration Tasks

When the routers are connected by PSTN through the asynchronous serial interface or by ISDN interface (such as BRI or PRI) through ISDN network, the DDR is applied. When there are packets needed to be sent, the routers set up connection and send packets, otherwise, there is no connection between them. When the idle time exceeds the defined time, the routers will disconnect. SO DDR is a very economical dial-up method. Please perform the tasks in the following sections to configure DDR configuration.

1)Configuring dialer interface

2)Configuring interface encapsulation, the default value is PPP.

3)Configuring DDR

Please refer to the section “Dialer Configuration Example” later in this chapter to understand the configuration of dial. Please refer to “WANs Command Reference” for dialer command. For the detailed configuration of link layer, network layer protocol and route protocol, please see the related chapters.

#### 8.4 DDR configuration command list

Global Configuration Command

**interface dialer** *number* ;

Interface Configuration Command

**dialer-group** *number*  
**dialer rotary-group** *number*  
**dialer string** *dialer-string*  
**dialer load-threshold** *enable\_threshold disable\_threshold*  
**dialer enable-timeout** *seconds*  
**dialer idle-timeout** *seconds*  
**dialer fast-idle** *seconds*  
**dialer priority** *number*  
**dialer dtm**

## 8.5 Configuring an Interface to Send and Receive calling

### 1. Send call to an interface and accept call from the one

In command to send call to an interface and accept call from the one, you can perform the configuration tasks below with PPP encapsulation.

- enter physical interface configuration mode `interface interface-type interface-number`

```
[DEFAULT@Router /config/]#interface
```

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

(08)Multilink Multilink-group interface

(09)Virtual-template Virtual template interface

(10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): 2 (select serialinterface)

Please input a interface name:s2/0

Will you excute it? (Y/N):y

- configuring the dialer method: **line dial**

Key Word:

Q(quit)

(00)backup Modify backup parameters

(01)bandwidth Set the interface bandwidth

(02)chinese help message in Chinese

(03)chmem Change memory of system

(04)clear\_drv clear interface statistic counter

(05)crypto Encryption module

(06)custom-queue-list Assign a custom queue list to interface

(07)default restore default configuration

(08)delay Set the interface delay

(09)description Set the interface description

(10)dsr-ignore ignore dsr signal

(11)encapsulation Set encapsulation type for an interface

(12)english help message in English

(13)exit exit / quit

(14)fair-queue enable fair queue on interface  
(15)hdlc-transparent Set this interface in hdlc transparent mode  
(16)hdlc-udp-tunnel Set IP address and UDP port of source and destination  
(17)help Description of the interactive help system  
(18)history look up history  
(19)interface interface configuration  
(20)ip IP configuration commands  
(21)keep-alive Set the interval of sending link check frame  
(22)line Configure dialing mode  
(23)mtu Set the interface MTU  
(24)no negate configuration  
(25)pdp pdp configuration commands  
(26)physical-layer Configure physical layer parameters  
(27)priority-group Assign a priority group to interface  
(29)random-detect enable weighted random early detect on interface  
(30)router routing protocol configuration  
(31)service-policy Assign a priority group to interface  
(32)show show configuration and status  
(33)shutdown Shutdown the current interface  
(34)snmp Modify SNMP interface parameters

Please Input the code of command to be excute(0-34): 22 (select line)

Key Word:

U(undo) D(default) Q(quit)

(00)dial Set dial-line

(01)leased Set leased-line

Please Input the code of command to be excute(0-1): 0 (select dial)

Will you excute it? (Y/N):y

- configuring ip address: **ip address** *ip-address* [ *net-mask* ]

Key Word:

Q(quit)

(00)backup Modify backup parameters

(01)bandwidth Set the interface bandwidth

(02)chinese help message in Chinese

(03)chmem Change memory of system

(04)clear\_drv clear interface statistic counter

(05)crypto Encryption module

(06)custom-queue-list Assign a custom queue list to interface

(07)default restore default configuration

(08)delay Set the interface delay

(09)description Set the interface description

(10)dialer Dial-on-demand routing (DDR) commands

(11)dialer-group Assign interface to dialer-list

(12)dsr-ignore ignore dsr signal

(13)encapsulation Set encapsulation type for an interface

(14)english help message in English

(15)exit exit / quit

(16)fair-queue enable fair queue on interface

(17)hdlc-transparent Set this interface in hdlc transparent mode

```

(18)hdlc-udp-tunnel Set IP address and UDP port of source and destination
(19)help Description of the interactive help system
(20)history look up history
(21)interface interface configuration
(22)ip IP configuration commands
.....
Please Input the code of command to be excute(0-37):22 (select command ip)
Key Word:
U(undo) D(default) Q(quit)
(00)access-group Specify access control for packets
(01)address IP address
(02)beigrp Enhanced Interior Gateway Routing Protocol
.....
Please Input the code of command to be excute(0-21): 1 (select address)
Input 1 ,select address
Key Word:
Q(quit)
(00)A.B.C.D IP address
(01)negotiated IP address negotiated over PPP or via DHCP
Please Input the code of command to be excute(0-1): 0
Input 0 ,select the option A.B.C,D
Please input a IP Address:192.168.19.80
note : Input the IP address here, 192.168.19.80 is noly a example.
Key Word:
Q(quit)
(00)A.B.C.D IP netmask
Please Input the code of command to be excute(0-0): 0
Please input a IP Address:255.255.255.0
Key Word:
Q(quit)
(00)secondary Make this IP address a secondary address
(01)<cr>
Please Input the code of command to be excute(0-1): 1
Will you excute it? (Y/N):y

```

- configuring **dialer map**: **dialer map** *next-hop-address* [ **name** *hostname* ] [ **broadcast** ] [ *dialer-string* ]

```

Key Word:
Q(quit)
(00)backup Modify backup parameters
(01)bandwidth Set the interface bandwidth
(02)chinese help message in Chinese
(03)chmem Change memory of system
(04)clear_drv clear interface statistic counter
(05)crypto Encryption module
(06)custom-queue-list Assign a custom queue list to interface
(07)default restore default configuration
(08)delay Set the interface delay
(09)description Set the interface description

```

## (10)dialer Dial-on-demand routing (DDR) commands

.....

Please Input the code of command to be excute(0-37):10 (select command dialer)

Key Word:

U(undo) D(default) Q(quit)

(00)called Dialer called string

(01)caller Dialer caller string

.....

(07)map Define multiple dial-on-demand numbers

(08)priority Set interface priority in dialer rotary group

(09)rotary-group Add this interface to a dialer rotary group

(10)string Set default telephone number

(11)wait-for-carrier-time Set the router wait for carrier time

Please Input the code of command to be excute(0-11): 7 (select map)

Key Word:

Q(quit)

(00)A.B.C.D IP address

Please Input the code of command to be excute(0-0): 0

Input 0 , select option A.B.C.D

Please input aIP Address:192.168.19.80 ( Input IP address,for example: 192.168.19.80 )

Key Word:

Q(quit)

(00)WORD Dialer string

(01)broadcast Broadcast to this address

(02)class Dialer map class

(03)modem-script Specify modem dialing script

(04)name Map to a host

(05)system-script Specify system dialing script

Please Input the code of command to be excute(0-5): 4 (select name)

Key Word:

Q(quit)

(00)WORD Host name to map

Please Input the code of command to be excute(0-0): 0

Input 0 , select WORD

Please input a string:NAME ( Input host computer name,for example:NAME )

Key Word:

Q(quit)

(00)WORD Dialer string

(01)broadcast Broadcast to this address

(02)class Dialer map class

(03)modem-script Specify modem dialing script

(04)system-script Specify system dialing script

Please Input the code of command to be excute(0-4): 1

Input 1 , select broadcast

Key Word:

Q(quit)

(00)WORD Dialer string

(01)class Dialer map class

```
(02)modem-script Specify modem dialing script
(03)system-script Specify system dialing script
Please Input the code of command to be excute(0-3): 0
Input 0 , select WORD
Please input a string:2
note : Input dialer string here,for example,2.
Will you excute it? (Y/N):y
```

## 2. Send calls to several interfaces and accept calls from them

In command to send calls to several interfaces and accept calls from them, you can perform the configuration tasks below.

- enter physical interface configuration mode `interface interface-type interface-number`  
(pls see the above section send call to an interface and accept call from the one for concrete configuration)
- configuring the dialer method: **line dial**  
(pls see the above section send call to an interface and accept call from the one for concrete configuration)
- configuring **ip address**: `ip address ip-address [ net-mask ]`  
(pls see the above section send call to an interface and accept call from the one for concrete configuration)
- configuring **dialer map**: `dialer map next-hop-address [ name hostname ] [ broadcast ] dialer-string`  
(pls see the above section send call to an interface and accept call from the one for concrete configuration)
- configuring several **dialer maps list**

## 3. Configuring dialer with dialer interface

- Define dialer interface corresponding to the dialer, the command is: *interface dialer* number

```
[DEFAULT@Router config]#interface
```

Key Word:

```
U(undo) D(default) Q(quit)
```

```
(00)FastEthernet FastEthernet interface
```

```
.....
```

```
(07)Dialer Dialer interface
```

```
(08)Multilink Multilink-group interface
```

```
(09)Virtual-template Virtual template interface
```

```
(10)Virtual-tunnel Virtual tunnel interface
```

```
Please Input the code of command to be excute(0-10): 7 (select Dialer interface)
```

```
Please input a interface name:d3
```

```
Note:input interface name here.
```

```
Will you excute it? (Y/N):y
```

- Configuring ip address to the dialer rotary group: `ip address ip-address [ net-mask ]`

Key Word:

```
Q(quit)
```

```
(00)bandwidth Set the interface bandwidth
```

```
(01)chinese help message in Chinese
```

```
(02)chmem Change memory of system
```

```
(03)clear_drv clear interface statistic counter
```

```
(04)crypto Encryption module
```

```
(05)default restore default configuration
```

(06)delay Set the interface delay  
 (07)description Set the interface description  
 (08)dialer Dial-on-demand routing (DDR) commands  
 (09)dialer-group Assign interface to dialer-list  
 (10)english help message in English  
 (11)exit exit / quit  
 (12)help Description of the interactive help system  
 (13)history look up history  
 (14)interface interface configuration  
 (15)ip IP configuration commands  
 (16)mtu Set the interface MTU

.....  
 Please Input the code of command to be excute(0-28): 15 (select command ip)

Key Word:  
 U(undo) D(default) Q(quit)  
 (00)access-group Specify access control for packets  
 (01)address IP address  
 (02)beigrp Enhanced Interior Gateway Routing Protocol

.....  
 Please Input the code of command to be excute(0-18): 1 (select address)

Key Word:  
 Q(quit)  
 (00)A.B.C.D IP address  
 (01)negotiated IP address negotiated over PPP or via DHCP

Please Input the code of command to be excute(0-1): 0

Please input a IP Address:192.168.19.80

Key Word:  
 Q(quit)  
 (00)A.B.C.D IP netmask

Please Input the code of command to be excute(0-0): 0

Please input a IP Address:255.255.255.0

Key Word:  
 Q(quit)  
 (00)secondary Make this IP address a secondary address  
 (01)<cr>

Please Input the code of command to be excute(0-1): 1

Will you excute it? (Y/N):y

- Configuring dialer map: dialer map next-hop-address [ name hostname ] [ broadcast ] dialer-string

Key Word:  
 Q(quit)  
 (00)bandwidth Set the interface bandwidth  
 (01)chinese help message in Chinese  
 (02)chmem Change memory of system  
 (03)clear\_drv clear interface statistic counter  
 (04)crypto Encryption module  
 (05)default restore default configuration  
 (06)delay Set the interface delay  
 (07)description Set the interface description  
 (08)dialer Dial-on-demand routing (DDR) commands

```
(09)dialer-group Assign interface to dialer-list
.....
Please Input the code of command to be excute(0-28): 8 (select command dialer )
Key Word:
U(undo) D(default) Q(quit)
(00)called Dialer called string
.....
(07)map Define multiple dial-on-demand numbers
(08)remote-name Specify remote name
(09)rotor Set outbound rotor order
(10)string Set default telephone number
(11)wait-for-carrier-time Set the router wait for carrier time
Please Input the code of command to be excute(0-11): 7 (select command map)
Key Word:
Q(quit)
(00)A.B.C.D      IP address
Please Input the code of command to be excute(0-0): 0
Input 0 ,select option A.B.C.D
Please input a IP Address:192.168.19.80
note : Input IP address here,for example: 192.168.19.80
Key Word:
Q(quit)
(00)WORD        Dialer string
(01)broadcast   Broadcast to this address
(02)class       Dialer map class
(03)modem-script Specify modem dialing script
(04)name        Map to a host
(05)system-script Specify system dialing script
Please Input the code of command to be excute(0-5): 4
Input 4 ,select name.
Key Word:
Q(quit)
(00)WORD      Host name to map
Please Input the code of command to be excute(0-0): 0
Input 0 ,select WORD
Please input a string:name
Key Word:
Q(quit)
(00)WORD Dialer string
(01)broadcast Broadcast to this address
(02)class   Dialer map class
(03)modem-script Specify modem dialing script
(04)system-script Specify system dialing script
Please Input the code of command to be excute(0-4): 1
Input 1 ,select broadcast
Key Word:
Q(quit)
(00)WORD Dialer string
(01)class Dialer map class
```

(02)modem-script Specify modem dialing script  
 (03)system-script Specify system dialing script  
 Please Input the code of command to be excute(0-3): 0 (select WORD)  
 Please input a string:2  
 note : input dialer string here,for example:2.  
 Will you excute it? (Y/N):y

- Attach the physical interface to dialer rotary group, enter the physical interface, dialer rotary-group dialer-interface, parameter dialer-interface is the dialer interface bound by the physical interface

Key Word:

Q(quit)  
 (00)bandwidth Set the interface bandwidth  
 (01)chinese help message in Chinese  
 (02)chmem Change memory of system  
 (03)clear\_drv clear interface statistic counter  
 (04)crypto Encryption module  
 (05)default restore default configuration  
 (06)delay Set the interface delay  
 (07)description Set the interface description  
 (08)dialer Dial-on-demand routing (DDR) commands  
 (09)dialer-group Assign interface to dialer-list

.....

Please Input the code of command to be excute(0-28): 8 (select command dialer)

Key Word:

U(undo) D(default) Q(quit)  
 (00)called Dialer called string  
 (01)caller Dialer caller string  
 (02)dtr Set DTR dialing for interface  
 (03)enable-timeout Set time interval between line down and dialing  
 (04)fast-idle Set idle time when line contention  
 (05)hold-queue Set output hold queue length  
 (06)idle-timeout Set idle time before disconnecting line  
 (07)map Define multiple dial-on-demand numbers  
 (08)priority Set interface priority in dialer rotary group  
 (09)rotary-group Add this interface to a dialer rotary group  
 (10)string Set default telephone number  
 (11)wait-for-carrier-time Set the router wait for carrier time  
 Please Input the code of command to be excute(0-11):9 (select rotary-group)

Input 9 ,select rotary-group

Key Word:

Q(quit)  
 (00)Dialer Dialer interface  
 Please Input the code of command to be excute(0-0): 0

Input 0 ,select Dialer

Please input a interface name:d3

note : input dialer interface name here,for example d3

Will you excute it? (Y/N):y

- The physical interface in the dialer rotary group will use the ip address of the dialer interface.

## 8.6 Customize the DDR Network

### 1. Set Line-Idle Time

To specify the amount of time a line will stay idle before it is disconnected by DDR.

Set the line-idle time: **dialer idle-timeout** *seconds*

```
[DEFAULT@router /config/]#interface
```

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

(08)Multilink Multilink-group interface

(09)Virtual-template Virtual template interface

(10)Virtual-tunnel Virtual tunnel interface

Please Input the code of command to be excute(0-10): 2 (select serial interface)

Please input ainterface name:s2/0

Will you excute it? (Y/N):y

Key Word:

Q(quit)

(00)bandwidth Set the interface bandwidth

(01)chinese help message in Chinese

(02)chmem Change memory of system

(03)clear\_drv clear interface statistic counter

(04)crypto Encryption module

(05)default restore default configuration

(06)delay Set the interface delay

(07)description Set the interface description

(08)dialer Dial-on-demand routing (DDR) commands

(09)dialer-group Assign interface to dialer-list

(10)english help message in English

(11)exit exit / quit

(12)help Description of the interactive help system

(13)history look up history

(14)interface interface configuration

(15)ip IP configuration commands

(16)mtu Set the interface MTU

(17)multilink Configure multilink parameters

(18)multilink-group Put interface in a multilink bundle

(19)no negate configuration

(20)pdp pdp configuration commands

(21)peer Peer parameters for point to point interfaces

(22)ppp Point-to-point protocol

(23)pulse-time Configure pulsing of DTR during reset

(25)router routing protocol configuration

(26)show show configuration and status

(27)shutdown Shutdown the current interface

(28)snmp Modify SNMP interface parameters

Please Input the code of command to be excute(0-28): 8 (select command dialer)

Key Word:

U(undo) D(default) Q(quit)

Key Word:

U(undo) D(default) Q(quit)

(00)called Dialer called string

(01)caller Dialer caller string

(02)dtr Set DTR dialing for interface

(03)enable-timeout Set time interval between line down and dialing

(04)fast-idle Set idle time when line contention

(05)hold-queue Set output hold queue length

(06)idle-timeout Set idle time before disconnecting line

(07)map Define multiple dial-on-demand numbers

(08)priority Set interface priority in dialer rotary group

(09)rotary-group Add this interface to a dialer rotary group

(10)string Set default telephone number

(11)wait-for-carrier-time Set the router wait for carrier time

Please Input the code of command to be excute(0-11): 6 (select idle-timeout)

Key Word:

Q(quit)

(00)<0-2147483> Idle timeout in seconds

Please Input the code of command to be excute(0-0): 0

Please input a digital number:2

note : input line-idle time here,for example 2.

Will you excute it? (Y/N):y

## 2. Set Idle Time for Busy Interfaces

When an interface has set up a link, another interface is need to set up a new link with it, that's called competition. If the line-idle time exceeds the specified amount of time, the current call is disconnected by DDR.

Key Word:

U(undo) D(default) Q(quit)

Key Word:

U(undo) D(default) Q(quit)

(00)called Dialer called string

(01)caller Dialer caller string

(02)dtr Set DTR dialing for interface

(03)enable-timeout Set time interval between line down and dialing

(04)fast-idle Set idle time when line contention

(05)hold-queue Set output hold queue length

(06)idle-timeout Set idle time before disconnecting line

(07)map Define multiple dial-on-demand numbers

(08)priority Set interface priority in dialer rotary group

(09)rotary-group Add this interface to a dialer rotary group

(10)string Set default telephone number

(11)wait-for-carrier-time Set the router wait for carrier time

Please Input the code of command to be excute(0-11):4 (select fast-idle)

Key Word:

Q(quit)

(00)<1-2147483> Fast idle time in seconds

Please Input the code of command to be excute(0-0): 0

Please input a digital number:2

note : input the idle time of busy interface here,for example 2.

Will you excute it? (Y/N):y

### 3. Set dialer timeout

To set the minimum length of time an interface stays down before it is available to dial again after a line is disconnected or fails.

Set line-down time: **dialer enable-timeout** *seconds*

Key Word:

U(undo) D(default) Q(quit)

(00)called Dialer called string

(01)caller Dialer caller string

(02)dtr Set DTR dialing for interface

(03)enable-timeout Set time interval between line down and dialing

(04)fast-idle Set idle time when line contention

(05)hold-queue Set output hold queue length

(06)idle-timeout Set idle time before disconnecting line

(07)map Define multiple dial-on-demand numbers

(08)priority Set interface priority in dialer rotary group

(09)rotary-group Add this interface to a dialer rotary group

(10)string Set default telephone number

(11)wait-for-carrier-time Set the router wait for carrier time

Please Input the code of command to be excute(0-11): 3 (select enable-timeout)

Key Word:

Q(quit)

(00)<1-2147483> enable-time in seconds

Please Input the code of command to be excute(0-0): 0

Input 0 ,select option <1-2147483>

Please input a digital number:2

Note : input dialer timeout here,for example 2.

Will you excute it? (Y/N):y

### 4. Set Wait Time of carrying interface data

Set Wait Time of carrying interface data: **dialer wait-for-carrier-time** *seconds*

Key Word:

U(undo) D(default) Q(quit)

Key Word:

U(undo) D(default) Q(quit)

.....

(09)rotary-group Add this interface to a dialer rotary group

(10)string Set default telephone number

(11)wait-for-carrier-time Set the router wait for carrier time

Please Input the code of command to be excute(0-11): 11 (select option wait-for-carrier-time)

Key Word:

Q(quit)

```
(00)<1-2147483> Wait for carrier time in seconds
Please Input the code of command to be excute(0-0): 0
Input 0 , select option <1-2147483>
Please input a digital number:2
Note : input waiting time here,for example 2.
Will you excute it? (Y/N):y
```

#### 5. Access Control to a DDR Interface

You can specify the packet filtering function of the DDR interface. The user can divide the packet through the DDR interface into two kinds by access control:

**valid packet:** Valid packet is the packet has passed the access control. When the DDR interface receives a valid packet, DDR sends the packet out through the line and clears the idle timeout if the corresponding line is connected. Otherwise, DDR sends call out.

**Invalid packet:** the packet hasn't passed the access control. When the DDR interface receives an invalid packet, DDR sends the packet out through the line and doesn't clear the idle timeout if the corresponding line is connected. Otherwise, DDR discards the packet without sending call out.

#### 6. Set the Physical Interface Priority of dialer rotary group

The using sequense of the interfaces is determined by the priority of itself.0—the lowest, 255—the highest, the default value is 0.

Specify the priority of the physical interface in the dialer rotary group: **dialer priority number**

Key Word:

```
U(undo) D(default) Q(quit)
```

Key Word:

```
U(undo) D(default) Q(quit)
```

.....

```
(08)priority Set interface priority in dialer rotary group
(09)rotary-group Add this interface to a dialer rotary group
(10)string Set default telephone number
(11)wait-for-carrier-time Set the router wait for carrier time
Please Input the code of command to be excute(0-11): 8 (select priority)
Key Word:
Q(quit)
(00)<0-255> Priority for dialing use
Please Input the code of command to be excute(0-0): 0
Please input a digital number:2 (set priority,for example 2.)
Will you excute it? (Y/N):y
```

#### 7. Specify the threshold value of the dialer rotary group

After the threshold value is specified, DDR will monitor the flow of the interface. When the flow exceeds the threshold and there is an usable interface in the dialer group, the interface will be turned on to add the bandwidth of the dialer group. When the flow under the threshold, the redundant interfaces will be disconnected automatically. If the physical interface is configured priority, the interface turned on or disconnected is determined according to the priority. The highest priority interface will be chosen when the interface is active, and lowest priority interface will be chosen when the interface is inactive.

Specify the threshold value of the dialer rotary group

**dialer load-threshold enable-threshold disable-threshold**

Key Word:

```
U(undo) D(default) Q(quit)
```

```
(00)called Dialer called string
```

```
(01)caller Dialer caller string
(02)enable-timeout Set time interval between line down and dialing
(03)fast-idle Set idle time when line contention
(04)hold-queue Set output hold queue length
(05)idle-timeout Set idle time before disconnecting line
(06)load-threshold Specify threshold for placing additional calls
(07)map Define multiple dial-on-demand numbers
(08)remote-name Specify remote name
(09)rotor Set outbound rotor order
(10)string Set default telephone number
(11)wait-for-carrier-time Set the router wait for carrier time
Please Input the code of command to be excute(0-11): 6 (select option load-threshold)
```

Key Word:

Q(quit)

```
(00)<0-100> Load threshold to place another call
```

Please Input the code of command to be excute(0-0): 0

Input 0 ,select option <0-100>

Please input a digital number:3

note : input the active threshold value here,for example 3

Key Word:

Q(quit)

```
(00)<0-100> Load threshold to disconnect a call
```

Please Input the code of command to be excute(0-0): 0

input 0 ,select option <0-100>

Please input a digital number:2

note : input the inactive threshold value here,for example 2.

Will you excute it? (Y/N):y

## 8. Specify the dtr method as the dialer method

You can directly activate the dialer when the DTR signal is valid in the DTE.

Specify the dtr as the dialer method

### **dialer dtr**

```
(00)called Dialer called string
(01)caller Dialer caller string
(02)dtr Set DTR dialing for interface
(03)enable-timeout Set time interval between line down and dialing
(04)fast-idle Set idle time when line contention
(05)hold-queue Set output hold queue length
(06)idle-timeout Set idle time before disconnecting line
(07)map Define multiple dial-on-demand numbers
(08)priority Set interface priority in dialer rotary group
(09)rotary-group Add this interface to a dialer rotary group
(10)string Set default telephone number
(11)wait-for-carrier-time Set the router wait for carrier time
Please Input the code of command to be excute(0-11): 2 (select dtr)
Will you excute it? (Y/N):y
```

## 9. Create a dialer hold queue to the dialer interface

The packets destined for DDR interface are discarded if no connection exists, after creating hold queue, the packets

won't be discarded before the connection is created

Specify the dialer hold queue to the dialer interface **dialer hold-queue** *packet-number*

(00)called Dialer called string  
(01)caller Dialer caller string  
(02)dtr Set DTR dialing for interface  
(03)enable-timeout Set time interval between line down and dialing  
(04)fast-idle Set idle time when line contention  
(05)hold-queue Set output hold queue length  
.....

Please Input the code of command to be excute(0-11): 5 (select option hold-queue)

Key Word:

Q(quit)

(00)<0-100> Specify size of output hold queue

Please Input the code of command to be excute(0-0): 0

Input 0 ,select option <0-100>

Please input a digital number:2

note : specify hold queue here,for example 2.

Will you excute it? (Y/N):y

## 8.7 Monitoring and Maintaining the Dialer Connection

Display the DDR interface information **show dialer interface** *type number*

[DEFAULT@router /config/]#show

Key Word:

U(undo) D(default) Q(quit)

(00)alias alias for command  
(01)arp ARP table  
(02)backup Backup status  
(03)board-info Board information  
(04)break router breakpoint information  
(05)  
(06)class-map show class-map configuration  
(07)configuration show configuration in flash memory  
(08)controller Interface controller status  
(09)cpu cpu usage information  
(10)debug State of each debugging option  
(11)dhcp DHCP information  
(12)dialer Dialer parameters and statistics

MORE

12

input 12 ,select dialer

Key Word:

Q(quit)

(00)interface Show dialer information on one interface  
(01)maps Show dialer maps  
(02)sessions Show dialer sessions

Please Input the code of command to be excute(0-2): 0

Input 0 ,select interface

Key Word:

Q(quit)

```
(00)Serial Serial interface
(01)Async Asynchronous interface
(02)Dialer Dialer interface
Please Input the code of command to be excute(0-2): 0
Input 0 ,select option Serial
Please input a interface name:s2/0
note :Input the interface name here,for example S2/0.
Will you excute it? (Y/N):y
screen will display the information similar to below:
```

```
Serial2/0 - dialer type = DTR
Idle timer (2 secs), Fast idle timer (2 secs)
Wait for carrier (2 secs), Re-enable (2 secs)
Dial String Successes Failures Last called Last status
* 0 0 never
Dialer state is Line down
```

explanation of displayed information are as follows:

|                  |                                                |
|------------------|------------------------------------------------|
| Dialer_Strings   | corresponding dialer strings in the dialer map |
| Successes        | number of dialer map call successes            |
| Failures         | number of dialer map call failures             |
| Last_call        | using time in the dialer map last call         |
| Idle timer       | set time with dialer idle-timeout command      |
| Fast Idle timer  | set time with Dialer fast-idle command         |
| Wait for carrier | set time with Dialer wait-for-carrier command  |
| Re_enable        | set time with dialer enable-timeout command    |

## 8.8 Dailer Configuration Example

### 8.8.1 The example of dialing to Multiple points

```
interface s1/1
ip address 131.108.126.1 255.255.255.0
dialer wait-for-carrier-time 100
dialer map 131.108.126.10 5558899
dialer map 131.108.126.15 5555555
```

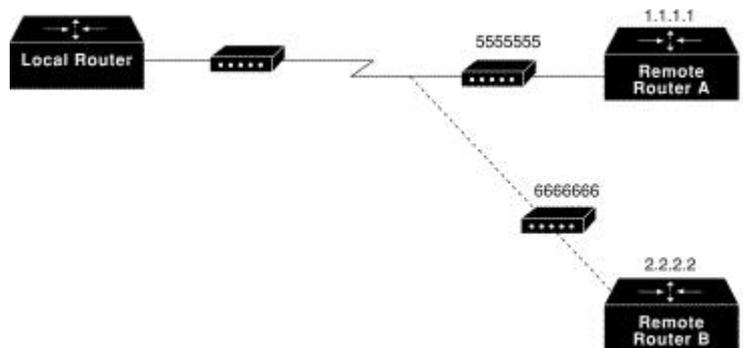
### 8.8.2 Configuring Dialer Rotary Groups Example

The example below defines the dialer-interface, and attaches the serial1/1 and serial1/2 to dialer interface.

```
interface dialer 1
ip address 131.108.2.1 255.255.255.0
ip address 131.126.2.1 255.255.255.0 secondary
dialer map 131.108.2.5 1234567
dialer map 131.126.2.55 7654321
! Interfaces serial 1 and 2 are placed in dialer rotary group 1. All of
! the interface configuration commands
! applied to interface dialer 1 apply to these interfaces.
interface serial1/1
dialer rotary-group dialer 1
interface serial1/2
dialer rotary-group d1
```

### 8.8.3 The examples of dialing to one or multiple points with dialer map

as the following figure



If local router only need dial to Router A, you can use command *dialer string* configure 55555555 to the dialer string, the configuration is described as follows:

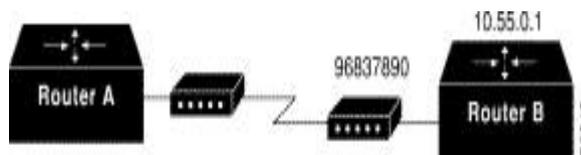
```
interface serial1/1
dialer string 5555555
```

If local router need dial to multiple points, you must configure dialer map. Otherwise, the router can't distinguish the dialer number of the different destinations. The configuration is described as follows:

```
interface serial 1/1
dialer map 1.1.1.1 5555555
dialer map 2.2.2.2 6666666
```

### 8.9 Script Configuration Example

Router A need dial to Router B



```
chat-script dial ABORT ERROR "" "AT Z" OK "ATDT \T" TIMEOUT 30 CONNECT \c
interface async 0/0
dialer map 10.55.0.1 modem-script dial 96837890
```

Script Example:

Dialer script is not only to use for launch calling to Modem, but also to use for automatic register to the remote DTE after dial-on. Thus, the dialer script can be divided into Modem script and registration script based on the different targets. The two kind scripts use the same script language but with different target. The following script language is compatible with UNIX dialer script language, which includes the following features:

- The content of script is capital sensitive, such as ABORT is different character string form abort.
- The script consists of some pre-specified keywords and sending/waiting character string sequenced aggregation. The waiting character string pair start from sending character, except keywords.
- the characters that are all included in the double quotation marks("") is treated as a full character string.
- Separate the character string by space.
- Automatic attaching an Enter symbol for each sending character string, except ending as \c.
- The match method of receiving content and waiting character string is random.

#### 8.9.1 Modem Script Execution Example

| Expected and Sending Character String Pair | Execution                                                        |
|--------------------------------------------|------------------------------------------------------------------|
| ABORT ERROR                                | End the script execution if the text "ERROR" is found.           |
| " " "AT Z"                                 | Without expecting anything, send an "AT Z" command to the modem. |

|              |                                                                                   |
|--------------|-----------------------------------------------------------------------------------|
| CONNECT \c   | Expect "connect," but do not send anything.                                       |
| TIMEOUT 30   | Specify the exceeding time of receiving expected character strings as 30 seconds. |
| OK "ATDT \T" | Wait to see "OK." Sending dialer string.                                          |

After the modem script is successfully executed, the login script is executed. The examples of executing logging script are as below.

### 8.9.2 Login Script Execution Example

| Expected and Sending Character String Pair | Execution                                                           |
|--------------------------------------------|---------------------------------------------------------------------|
| ABORT invalid                              | End the script execution if the message "invalid " is displayed.    |
| TIMEOUT 15                                 | Wait up to 15 seconds.                                              |
| Name: myname                               | send login name while "name" appeared in received character string. |
| Word: mypassword                           | send password while "word" appeared in received character string.   |

## 9. interface backup configuration

This chapter will describe how to configure the interface backup function. the interface backup function executed on asynchronism serial, synchronism serial and ISDN interface are also included.

Please refer to the 《[interface backup command reference](#)》 for the full description of interface backup function.

### 9.1 realization information

Interface backup function can launch backup interface or close it based on the primary interface status and flow information. when the primary interface is down because of the line, the backup interface will be activated automatically. the data sent or received through primary interface before can be sent or received through backup interface to realize the router, which enhanced the connection reliability between the destination and source router. When the primary interface flow is too large, the backup interface can be activated, which realize parts of data sent through backup interface for accelerating data transferring. however, if the primary interface status transfer from down to up or both primary and backup interface flow are low, the backup interface can be inactive on backup status, not transferring data for saving the cost of line. the following physical interface type can be regarded as primary interface.

- asynchronism serial interface
- ISDN
- synchronism serial interface

Excepting the above three types, backup interface can also include the dialer logical interface.

### 9.2 interface backup configuration task list

Configure the interface backup function in the above interface types, execute the following tasks under the interface configuration mode.

select the backup interface

The below tasks can also be executed, they are optional, which provide many usage and enhance the interface backup function.

launch interface backup delay

launch flow equilibrium backup

### 9.3 launch backup function and select the backup interface

To realize the interface backup function, first configure the backup interface. The following commands can be used under interface command in the global configuration directory:

| command                    | function                     |
|----------------------------|------------------------------|
| backup interface slot/port | Select the backup interface. |

```
[DEFAULT@Router /config/]# interface
```

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

(05)Loopback Loopback interface

(06)Tunnel Tunnel interface

(07)Dialer Dialer interface

```
(08)Multilink      Multilink-group interface
(09)Virtual-template Virtual template interface
(10)Virtual-tunnel Virtual tunnel interface
Please Input the code of command to be excute(0-10): 0
note : Input the interface needs to configure backup here,for example fastEthernet.
Please input a interface name:f0/0
note : Input the interface name here,for example f0/0.
Will you excute it? (Y/N):y
```

Key Word:

Q(quit)

(00)arp set arp timeout

(01)backup Modify backup parameters

(02)bandwidth Set the interface bandwidth

.....

Please Input the code of command to be excute(0-35): 1 (select backup)

Key Word:

U(undo) D(default) Q(quit)

(00)delay Delays before backup line up or down transitions

(01)interface Configure an interface as a backup

(02)load Load thresholds for line up or down transitions

(03)always Second interface always Up when primary interface down(dialer)

Please Input the code of command to be excute(0-3): 1

Input 1 ,select interface :

Key Word:

Q(quit)

(00)Serial Serial interface

(01)Async Asynchronous interface

Please Input the code of command to be excute(0-1): 0

note : Input backup interface here,for example Serial.

Please input a interface name:s2/0

<![endif]>note : Input interface name here,for example s2/0

Will you excute it? (Y/N):y

#### 9.4 launch interface backup delay

configure backup interface launching and closing delay,which realize the time difference between the primary interface status changing and backup interface status changing.

First step,select backup interface.

Second step,launch interface backup delay

select backup interface,using the following commands under interface configuration mode.

| command                    | function                    |
|----------------------------|-----------------------------|
| backup interface slot/port | select the backup interface |

```
[DEFAULT@Router /config/]# interface
```

Key Word:

U(undo) D(default) Q(quit)

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

```

.....
Please Input the code of command to be excute(0-10): 0
note : Input the interface needs to configure backup here,for example Fast Ethernet.
Please input a interface name:f0/0
note : Input the interface name here,for example f0/0.
Will you excute it? (Y/N):y
Key Word:
Q(quit)
(00)arp set arp timeout
(01)backup Modify backup parameters
(02)bandwidth Set the interface bandwidth
.....
Please Input the code of command to be excute(0-35): 1 (select backup)
Key Word:
U(undo) D(default) Q(quit)
(00)delay Delays before backup line up or down transitions
(01)interface Configure an interface as a backup
(02)load Load thresholds for line up or down transitions
(03)always Second interface always Up when primary interface down(dialer)
Please Input the code of command to be excute(0-3): 1
Input 1 ,select interface :
Key Word:
Q(quit)
(00)Serial Serial interface
(01)Async Asynchronous interface
Please Input the code of command to be excute(0-1): 0
<![endif]>note : Input backup interface here,for example Serial.
Please input a interface name:s2/0
<![endif]>note : Input interface name here,for example s2/0.
Will you excute it? (Y/N):y

```

| command                                                          | function                                             |
|------------------------------------------------------------------|------------------------------------------------------|
| backup delay {enable-delay   never }<br>{disable-delay   never } | define backup interface active and<br>inactive delay |

```

Launch interface backup delay,choosing command backup under the configure interface directory.
Key Word:
U(undo) D(default) Q(quit)
(00)delay Delays before backup line up or down transitions
(01)interface Configure an interface as a backup
(02)load Load thresholds for line up or down transitions
(03)always Second interface always Up when primary interface down(dialer)
Please Input the code of command to be excute(0-3): 0
Input 0 ,select delay :
Key Word:
Q(quit)
(00)<0-4294967294> Activate Seconds

```

```
(01)never          Never activate the backup line
Please Input the code of command to be excute(0-1): 0
note : Select whether the activate delay is needed or not here,for example 0.
<![endif]>Please input a digital number:Please input a string:34
note : If selecting avtivate delay,input time here,for example 34.
Key Word:
Q(quit)
(00)<0-4294967294> Deactive Seconds
(01)never Never deactivate the backup line
Please Input the code of command to be excute(0-1): 0
note : Determine whether disactivate delay is needed or not here,for example 0.
Please input a digital number:Please input a string:23
note : If choosing disactivate delay,input time here,for example 23.
Will you excute it? (Y/N):y
```

### 8.10 launch flow equilibrium backup

When the actual flow of primary interface exceeds the percent threshold,the backup interface will be activated entering working status. However,when the ratio of the primary and backup interface actual flow with primary interface bandwidth is lower than setting threshold,the backup interface will be disactivated and enter backup status.

launch flow equilibrium backup,the following tasks are needed:

First step,select backup interface.

Second step,launch flow equilibrium on this interface.

first step,select backup interface.execute commands under interface configuration.

| command                    | function                    |
|----------------------------|-----------------------------|
| backup interface slot/port | select the backup interface |

```
[DEFAULT@Router /config/]# interface
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)FastEthernet  FastEthernet interface
(01)Ethernet      Ethernet interface
(02)Serial        Serial interface
(03)Async         Asynchronous interface
(04)Null          Null interface
(05)Loopback     Loopback interface
(06)Tunnel        Tunnel interface
(07)Dialer        Dialer interface
(08)Multilink     Multilink-group interface
(09)Virtual-template Virtual template interface
(10)Virtual-tunnel Virtual tunnel interface
Please Input the code of command to be excute(0-10): 0
note : Input the interface needs to configure backup here,for example FastEthernet.
Please input a interface name:f0/0
note : Input interface name here,for example f0/0.
Will you excute it? (Y/N):y
```

Key Word:

Q(quit)

(00)arp set arp timeout

(01)backup Modify backup parameters

(02)bandwidth Set the interface bandwidth

.....

Please Input the code of command to be excute(0-35): 1 (select backup)

Key Word:

U(undo) D(default) Q(quit)

(00)delay Delays before backup line up or down transitions

(01)interface Configure an interface as a backup

(02)load Load thresholds for line up or down transitions

(03)always Second interface always Up when primary interface down(dialer)

Please Input the code of command to be excute(0-3): 1

Input 1 ,select interface :

Key Word:

Q(quit)

(00)Serial Serial interface

(01)Async Asynchronous interface

Please Input the code of command to be excute(0-1): 0

<![endif]>note : Input backup interface here,for example Serial.

Please input a interface name:s2/0

<![endif]>note : Input interface name here,for example s2/0.

Will you excute it? (Y/N):y

second step,launch flow equilibrium on the interface.execute the following command under interface configuration.

| command                                                                | function                                                                                    |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| backup load {enable-threshold   never }<br>{disable-threshold   never} | activate or deactivate backup interface threshold through configuring interface backup flow |

Key Word:

Q(quit)

(00)arp set arp timeout

(01)backup Modify backup parameters

(02)bandwidth Set the interface bandwidth

.....

Please Input the code of command to be excute(0-35): 1 (select backup)

Key Word:

U(undo) D(default) Q(quit)

(00)delay Delays before backup line up or down transitions

(01)interface Configure an interface as a backup

(02)load Load thresholds for line up or down transitions

(03)always Second interface always Up when primary interface down(dialer)

Please Input the code of command to be excute(0-3): 2

Input 2 ,select load :

Key Word:

Q(quit)

(00)<0-100> Activate Percentage

```
(01)never      Never activate the backup line
Please Input the code of command to be excute(0-1): 0
note : Determine whether activating backup interface threshold is needed or not here,for example 0.
Please input a digital number:Please input a string:23
note : If choosing activate threshold,input threshold here,for example 23.
Key Word:
Q(quit)
(00)<0-100> Deactive Percentage
(01)never Never dectivate the backup line
Please Input the code of command to be excute(0-1): 0
note : Determine whether disactivating backup interface threshold is needed or not here,for example 0.
Please input a digital number:Please input a string:12
note : If choosing disactivate threshold,input threshold here,for example 12.
Will you excute it? (Y/N):y
```

### 8.11 interface backup configuration example

this section provide the PPP configuration example as below:

launch interface backup function on serial1/0 interface,choosing serial1/1 as backup interface. the time of backup interface activate delay and disactivate delay are both 5s.when the primary interface actual flow exceeds 60% bandwidth,flow equilibrium will activate backup interface,otherwise when both interfaces actual flow lower than 30% bandwidth, flow equilibrium will disactivate backup interface.

```
configure router
  interface s1/0
    backup interface int s1/1
    backup delay 5 5
    backup load 70 30
```

when the primary interface is down,the dialer backup interface will be on connecting.

if primary interface choosing normal dialer interface as backup,when the primary interface protocol is down and the backup interface is not needed to send data,backup dialer interface will not dial automatically until sending data.if this command is set,no matter whether there is data need to transfer,the backup interface will setup dial connection immediatly based on the primary interface protocol is down.(applied to connection slow setup normal dialer interface as backup)

launch flow equilibrium backup,execute below tasks:

First step,choosing backup interface.

Second step, once the primary interface protocol is down,the backup interface will dial at once on this interface.

first step,choosing backup interface.execute below command under interface configuration.

| command                    | function                |
|----------------------------|-------------------------|
| backup interface slot/port | select backup interface |

```
[DEFAULT@Router /config/# interface
```

Key Word:

```
U(undo) D(default) Q(quit)
(00)FastEthernet  FastEthernet interface
(01)Ethernet      Ethernet interface
(02)Serial        Serial interface
(03)Async         Asynchronous interface
```

```

.....
Please Input the code of command to be excute(0-10): 0
note : Input interface needs to configure backup here,for example Fast Ethernet.
Please input a interface name:f0/0
note : Input interface name here,for example f0/0.
Will you excute it? (Y/N):y
Key Word:
Q(quit)
(00)arp set arp timeout
(01)backup Modify backup parameters
(02)bandwidth Set the interface bandwidth

```

```

.....
Please Input the code of command to be excute(0-35): 1 (select backup)
Key Word:
U(undo) D(default) Q(quit)
(00)delay Delays before backup line up or down transitions
(01)interface Configure an interface as a backup
(02)load Load thresholds for line up or down transitions
(03)always Second interface always Up when primary interface down(dialer)
Please Input the code of command to be excute(0-3):1

```

```

Input 1 ,select interface :
Key Word:
Q(quit)
(00)Serial Serial interface
(01)Async Asynchronous interface
Please Input the code of command to be excute(0-1): 0
<![endif]>note : Input backup interface here,for example Serial.
Please input a interface name:s2/0
<![endif]>note : Input interface name here,for example s2/0.
Will you excute it? (Y/N):y

```

second step,once the primary interface protocol is down,the backup interface will dial immediately on this interface.execute the command under interface configuration.

| command       | function                                                                     |
|---------------|------------------------------------------------------------------------------|
| backup always | backup interface always setup connection to primary interface protocol down. |

```

Key Word:
Q(quit)
(00)arp set arp timeout
(01)backup Modify backup parameters
(02)bandwidth Set the interface bandwidth
.....
Please Input the code of command to be excute(0-35): 1 (select backup)
Key Word:
U(undo) D(default) Q(quit)
(00)delay Delays before backup line up or down transitions
(01)interface Configure an interface as a backup
(02)load Load thresholds for line up or down transitions

```

(03)always Second interface always Up when primary interface down(dialer)

Please Input the code of command to be excute(0-3): 3

Input 3 , select always:

<![endif]>Will you excute it? (Y/N):y

this section provide configuration example as below(choosing a0/0 as a dialer interface):

**configure router**

interface s1/0

backup interface a0/0

backup always

## 9. IP Voice Configuration Task List

### 9.1 About Voice

D-Link 1700, 2600, 2700, 3600 Series support voice transmission. D-Link's voice support is implemented using voice packet technology. In voice packet technology, voice signals are packetized and transported in compliance with ITU-T specification H.323, which is the ITU-T specification for transmitting multimedia (voice, video, and data) across a local-area network. The introduction divided into three parts as below:

- About Voice Application
- Voice Primer
- About QoS

“About Voice Application” introduce the voice technology provided by D-Link voice device; “Voice Primer” give the brief description of voice technology for primary user; “About QoS” briefly introduce the principle of QoS.

### 9.2 About Voice Application

Voice over IP enables a D-LINK series router to carry voice traffic over an IP network. As the voice packets are transported by IP, you must configure the parameters relating to the voice interface and some particular functions (such as dial peer) .

### 9.3 Dial Peers

The key point to understanding D-Link Voice over IP functions is to understand dial peers. Each dial peer defines the characteristics associated with a call leg, as shown in Figure 1 and Figure 2. Four call legs make comprise and end-to-end call—two from the perspective of the source router as shown in Figure 1, and two from the perspective of the destination router as shown in Figure 2. Dial peers are used to apply attributes to call legs and to identify call origin and destination.

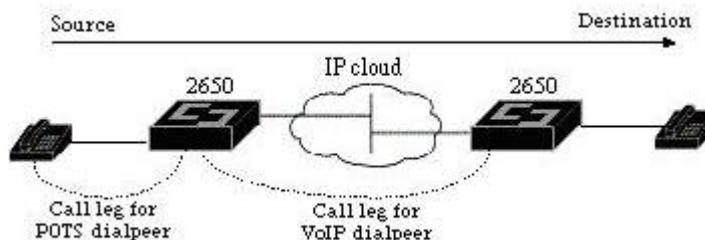


Figure 1 Dial Peer Call Legs from the Perspective of the Source IP Telephone Connector

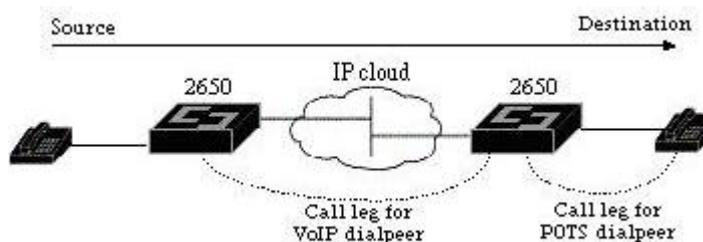


Figure 2 Dial Peer Call Legs from the Perspective of the Destination Router

There are two kinds of dial peer:

- POTS—Dial peer describing the characteristics of a traditional telephony network connection. POTS peers point to a particular voice port on a voice network device. To configure POTS dial peer, the key command that must be configureds are **config-port** and **config-destination-pattern**. The command **config-destination-pattern** defines the telephone number associated with this POTS dial peer. The command **config-port** associate this POTS dial peer with a specific voice port. Generally this command connects D-Link IP telephone equipments with telephone or local PBX telephone port.
- VoIP—Dial peer describing the characteristics of a packet network connection; in the case of Voice over IP, this is an IP network. VoIP peers point to specific VoIP devices. To configure VoIP dial peer, you must configure the

key commands **config-destination-pattern** and **set-session**. The command **config-destination-pattern** defines the destination telephone number associated with this VoIP dial peer. The command **set-session** specifies a destination IP address for this dial peer.

## 9.4 Voice Port

Use the voice port command of D-LinkIP telephone equipments to define the parameter about specified voice port. D-LinkIP telephone equipments support three voice ports:

- FXO---Foreign Exchange Office interface. The FXO interface is an RJ-11 connector that allows a connection to be directed at the PSTN's central office (or to a standard PBX interface, if the local telecommunications authority permits). This interface is of value for off-premise extension applications.
- FXS---The Foreign Exchange Station interface. This interface is an RJ-11 connector that allows connection for basic telephone equipment, keysets, PBXs, and supplies ring, voltage, and dial tone.
- E&M---The "Ear and Mouth" interface (or "RecEive and TransMit") interface. This interface is an RJ-48 connector that allows connection for PBX trunk lines (tie lines).

D-Link IP telephone connector currently provides only analog voice ports. The type of signaling associated with these analog voice ports depend on the interface module installed into the device. For example, V100 has two FXS ports, DI-1750 series routers support two-ports FXS, FXO and E&M voice card. DI-3600 series router supports either a two-port or four-port voice network module (VNM) of FXS, FXO and E&M.

## 9.5 Voice Primer

To understand D-LINK's voice implementations, it helps to have some understanding of analog and digital transmission and signaling. This section provides some very basic, abbreviated voice telephony information as background to help you configure Voice over IP, which includes the following topics:

- Numbering Scheme
- Analog versus Digital
- CODECs
- Delay
- Jitter
- Echo
- Signaling
- 

## 9.6 Numbering Scheme

The standard PSTN is basically a large, circuit-switched network. It uses a specific numbering scheme, which complies to the ITU-T E.164 recommendations. In D-Link's voice implementations, numbering schemes are configured using the **config-destination-pattern** command. For numbering, D-Link provides the concrete suggestion, please refer to the description of command **config-destination-pattern**.

## 9.7 Analog versus Digital

Until recently, the telephone network was based on an analog infrastructure. Analog transmission is not particularly robust or efficient at recovering from line noise. Because analog signals degrade over distance, they need to be periodically amplified; this amplification boosts both the voice signal and ambient line noise, resulting in degradation of the quality of the transmitted sound.

In response to the limitations of analog transmission, the telephony network migrated to digital transmission using pulse code modulation (PCM) or adaptive differential pulse code modulation (ADPCM). In both cases, analog sound is converted into digital form by sampling the analog sound 8000 times per second and converting each sample into a numeric code.

## 9.8 CODECs

PCM and ADPCM are examples of "waveform" CODEC techniques. Waveform CODECs are compression techniques that exploit the redundant characteristics of the waveform itself. In addition to waveform CODECs, there are source CODECs that compress speech by sending only simplified parametric information about voice transmission; these CODECs require less bandwidth. Source CODECs include linear predicative coding (LPC), code-excited linear prediction (CELP) and multi-pulse, multi-level quantization (MP-MLQ).

Coding techniques are standardized by the ITU-T in its G-series recommendations. The most popular coding standards for telephony and voice packet are:

- G.711—Describes the 64-kbps PCM voice coding technique. In G.711, encoded voice is already in the correct format for digital voice delivery in the public switched telephone network (PSTN) or through PBXes.
- G.723.1—Describes a compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This CODEC has two bit rates associated with it: 5.3 and 6.3 kbps. The higher bit rate is based on ML-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on CELP and provides system designers with additional flexibility.
- G.726—Describes ADPCM coding at 40, 32, 24, and 16 kbps. ADPCM-encoded voice can be interchanged between packet voice, PSTN, and PBX networks if the PBX networks are configured to support ADPCM.
- G.728—Describes a 16-kbps low-delay variation of CELP voice compression. CELP voice coding must be translated into a public telephony format for delivery to or through the PSTN.

G.729—Describes CELP compression where voice is coded into 8-kbps streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM.

## 9.9 Mean Opinion Score

Each CODEC provides a certain quality of speech. The quality of transmitted speech is a subjective response of the listener. A common benchmark used to determine the quality of sound produced by specific CODECs is the mean opinion score (MOS). With MOS, a wide range of listeners judge the quality of a voice sample (corresponding to a particular CODEC) on a scale of 1 (bad) to 5 (excellent). The scores are averaged to provide the mean opinion score for that sample. Table 1 shows the relationship between CODECs and MOS scores.

| Compression Method  | Bit Rate (kbps) | Framing Size | MOS Result |
|---------------------|-----------------|--------------|------------|
| G.711 PCM           | 64              | 0.125        | 4.1        |
| G.726 ADPCM         | 32              | 0.125        | 3.85       |
| G.728 LD-CELP       | 16              | 0.625        | 3.61       |
| G.729 CS-ACELP      | 8               | 10           | 3.92       |
| G.729 x 2 Encodings | 8               | 10           | 3.27       |
| G.729 x 3 Encodings | 8               | 10           | 2.68       |
| G.729a CS-ACELP     | 8               | 10           | 3.7        |
| G.723.1 MP-MLQ      | 6.3             | 30           | 3.9        |
| G.723.1 ACELP       | 5.3             | 30           | 3.65       |

Table 1: Compression Methods and MOS Scores

Although it might seem logical from a financial standpoint to convert all calls to low-bit rate CODECs to save on infrastructure costs, you should exercise additional care when designing voice networks with low-bit rate compression. There are drawbacks to compressing voice. One of the main drawbacks is signal distortion due to multiple encodings (called tandem encodings). For example, when a G.729 voice signal is tandem encoded three times, the MOS score drops from 3.92 (very good) to 2.68 (unacceptable). Another drawback is CODEC-induced delay with low bit-rate CODECs.

## 9.10 Delay

One of the most important design considerations in implementing voice is minimizing one-way, end-to-end delay. Voice traffic is real-time traffic; if there is too long a delay in voice packet delivery, speech will be unrecognizable. Delay is inherent in voice-networking and is caused by a number of different factors. An acceptable delay is less than 200 milliseconds.

There are basically two kinds of delay inherent in today's telephony networks: propagation delay and handling delay. Propagation delay is caused by the characteristics of the speed of light traveling via a fiberoptic-based or copper-based media. Handling delay (sometimes called serialization delay) is caused by the devices that handle voice information. Handling delays have a significant impact on voice quality in a packetized network. CODEC-induced delays are considered a handling delay. Table 2 shows the delay introduced by different CODECs.

| CODEC           | Bit Rate(kbps) | Compression Delay(ms) |
|-----------------|----------------|-----------------------|
| G.711 PCM       | 64             | 0.75                  |
| G.726 ADPCM     | 32             | 1                     |
| G.728 LD-CELP   | 16             | 3 to 5                |
| G.729 CS-ACELP  | 8              | 10                    |
| G.729a CS-ACELP | 8              | 10                    |
| G.723.1 MP-MLQ  | 6.3            | 30                    |
| G.723.1 ACELP   | 5.3            | 30                    |

Table 2: Delays caused by different CODECs

Another processing delay is to generate the time voice packets want. With G729 Coder, DSP generates a frame per 10 milliseconds. Two frames are placed in a voice packet, so packet relay is 20 milliseconds.

Another source of processing relay is the time required for a packet to be forwarded into the output queue.

## 9.11 Jitter

Jitter is nother factor of delay. In VoIP networks where existing a diversity between the expecting receiving time and real receiving time of voice packets, jitter can become a problem which results in incontinuous voice flow. D-LINK IP telephone receiver have built-in dejitter buffering for voice rebroadcasting to compensate for a certain amount of jitter.

## 9.12 End-to-end Delay

It is not very difficult for those users who acquaint the end-to-end signal route / data route, the coding and decoding technique, and the payload size to understand end-to-to delay. Coder delay (5 milliseconds for G711 and G726, 10 milliseconds for G729), packeting delay, fixed network delay and the delay from the two ends to code/decode, compose the end-to-end connection delay.

## 9.13 Echo

Echo refers to that the user heard his own voice when communicating on phone receiver. It can be canceled with relevant timing. If echo overtops 25 milliseconds, it will worsen the voice and make the communicating pause. In a traditional telecom network, echo is usually generated by the non-matching of impedance switching from 4-wire network to 2-wire local loop, and is controled by echo-cancel. In a voice packet network, echo-cancel is embedded in the low speed coder/decoder and functions on every DSP. The echo-cancel must be limited by the time of waiting for echo accept. The time is usually called echo mark. Generally echo mark is 32 milliseconds.

## 9.14 About QoS

### 9.14.1 What is QoS

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. Network transfer can be controlled with QoS. QoS also provides services based on various policies and provides various services for different operations such as voice, video, etc.

### 9.14.2 End-to-End QoS Module

Service model refers to a series of end-to-end QoS functions. QoS software supports three kinds of service model: Best-Effort service, Integrated service (Intserv), Differentiated service (Diffserv).

### 9.14.3 Best-Effort Service

Best effort is a single service model in which an application sends data whenever it must, in any quantity, and without requesting permission or first informing the network. For best-effort service, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. The D-Link QoS feature that implements best-effort service is first-in, first-out (FIFO) queueing.

### 9.14.4 Integrated Service

Integrated service is a multiple service model that can accommodate multiple QoS requirements. In this model the application requests a specific kind of service from the network before it sends data. Explicit signalling makes the request. The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. It is also expected to send data that lies within its described traffic profile.

The network performs admission control, based on information from the application and available network resources. It also commits to meeting the QoS requirements of the application as long as the traffic remains within the profile specifications. The network fulfills its commitment by maintaining per-flow state and then performing packet classification, policing, and intelligent queueing based on that state.

D-Link QoS provide Controlled Load Service and Guaranteed Rate Service by Resource Reservation Protocol (RSVP). Controlled Load Service allow to apply lower delay and higher throughput even at the crowded period of network. D-Link QoS provide Weighted Fair Queuing to implement this target.

### 9.14.5 Differentiated Service

Differentiated service is a multiple service model that can satisfy differing QoS requirements. However, unlike the integrated service model, an application using differentiated service does not explicitly signal the router before sending data.

For differentiated service, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification occurs in different ways, for example, while using the IP Precedence bit settings in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queueing. D-Link QoS provides Weighted Random Early Detection, Custom Queue, and Priority Queue that use for transmit differentiated service.

## 9.15 QoS Signalling

D-Link QoS signalling provides a way for an end station or network node to communicate with, or signal, its neighbors to request special handling of certain traffic. QoS signalling is useful for coordinating the traffic handling techniques provided by other QoS features. It plays a key role in configuring successful overall end-to-end QoS service across your network. QoS signalling fully takes advantage of the Internet Protocol (IP). Either in-band (IP Precedence) or

out-of-band (RSVP) signalling is used to indicate that a particular QoS service is desired for a particular traffic classification.

D-LinkIP telephone equipment provides IP Precedence and RSVP. Each voice packet will be marked corresponding identifier.

Please see the correlative documents for complete information of QoS signalling.

## About DSP sensing switch signalling tone

### Sense

Command **sense cptone port slot\_num/port\_num dial dial\_string tone\_type freq\_type slot\_num/port\_num** is the port number to be sensed of signaling tone. **dial\_string** is the number to be dialed for sensing some signaling tone. **tone\_type** is the type of signaling tone to be sensed. There's 8 types of them, they are respectively called DIALTONE\_PBX ,DIALTONE\_EXT , LERTTONE\_PBX , ALERTTONE\_EXT , BUSYTONE\_PBX , BUSYTONE\_EXT , EMPTYTONE\_PBX and EMPTYTONE\_EXT. Each two of them forms a team and respectively express "dialing tone", "echo tone", "busy tone" and "idle tone" in turn. PBX indicates the PBX signaling tone directly connected dwith this PBX. EXT indicates the PBX signaling tone not directly connected with this PBX. Thereinto 4 types of PBX signaling tone are necessary configuration (National standard supports default values). The other 4 types are optional and can be configured up to 12, they are mostly used to configure "busy tone". **freq\_type** is type of frequency and is divided into single frequency and dual frequency. Please refer to PBX specification for detail.

The first signaling tone has 4 sets of arguments: **high\_freq** ( high frequency , 2001 is invalid value , used in single frequency. )、**low\_freq** ( low frequency ) , **time\_on** ( duration of wave crest )、**time\_off** ( duration of trough ) .

Then we will take the sensing of the four PBX signaling tone for an example to make a detailed description.

#### 1、 Dialing tone :

When sensing the dialing tone ( **tone\_type** is DIALTONE\_PBX or DIALTONE\_EXT ) , **dial\_string** can be set an arbitrary numeral string, but it won't take any effect. **time\_on** of the dialing tone is 300, **time\_off** is 1023 (invalid value).

#### 2、 Echo tone :

When sensing echo tone ( **tone\_type** is ALERTTONE\_PBX or ALERTTONE\_EXT ) , **dial\_string** must be a phone number of another port on the PBX connected with this DSP and it must not be occupied. Namely it has dialed through the corresponding number of current **dial\_string**.

#### 3、 Busy tone :

When sensing busy tone ( **tone\_type** 为 BUSYTONE\_PBX or BUSYTONE\_EXT ) , you should first hang up another phone (number is **dial\_string**) on the PBX connected with DSP port. Then you can process sensing with this command.

#### 4、 Idle tone :

When sensing idle tone ( **tone\_type** is EMPTYTONE\_PBX or EMPTYTONE\_EXT ) , you should configure **dial\_string** to be a phone number not existing on the PBX connected with this DSP port, and then use this command to process sensing. Some switch has no idle tone, then you can use busy tone instead of it and the result of sensing is consistent with busy tone. Here the idle tone of this PBX can be set and can be not.

When sensing EXT signaling tone, you can apply the similar method.

### Configure

It will enter into **cptone** configuration mode as configuring signaling tone (use command **cptone slot\_num**). The four signaling tone of PBX must be configured, otherwise it will take the default value. Dialing tone (DIALTONE\_PBX or DIALTONE\_EXT) is required to be configured only two parameters, **time\_on** and **time\_off** are system specified values (respectively to be 300 and 1023). Other signaling tone must be configured four parameters. If this switch is single frequency, then the high frequency will take the invalid value 2001.

After completing configuring and exiting from the configure mode, the current configuration just takes effect. All DSPs and ports on a same slot will take the same configuration. Therefore we suggest you use ports on different slots when connecting different switchs except that the parameters of the two switch signaling tone are consistent.

After completing configuring and saving them, current configuration will be always taken. Use command **default cptone slot\_num** to resume the default configuration of this slot signaling tone.

When configuring `cptone`, we suggest you first use the command `default cptone slot_num` to reset corresponding of a slot into default value before entering into `cptone` configure mode, or else after entering into configure mode the ext signaling tone configured will be added behind former ext signal, but pbx signaling tone will overlay the former configuration. If the `cptone` of this slot has no ext signaling tone, before configuring you needn't use command `default` to reset.

### 9.15.1 Configure Voice over IP

This chapter shows you how to configure Voice over IP (VoIP) on the D-LinkIP telephone equipments. VoIP is a protocol that carry voice traffic over an IP network. Voice over IP is primarily a software feature; V100 has the fixed FXS voice port, to use this feature on D-Link DI-1750 and DI-3660 router, you must install a voice network module (VNM) or a voice interface card, each of interface card corresponding a particular signaling type associated with a voice port.

Voice over IP offers the following benefits:

- Toll bypass
- Remote PBX presence over WANs
- Unified voice/data trunking
- POTS-Internet telephony gateways

### 9.15.2 How Voice over IP Processes a Telephone Call

Before configuring Voice over IP, it helps to understand what happens at an application level when you place a call using Voice over IP. The general flow of a two-party voice call using Voice over IP is as follows (FXS port):

1. The user picks up the handset; this signals an off-hook condition to the signaling application part of Voice over IP.
2. The session application part of Voice over IP issues a dial tone and waits for the user to dial a telephone number.
3. The user dials the telephone number; those numbers are accumulated and stored by the session application.
4. After enough digits are accumulated to match a configured destination pattern, the telephone number is mapped to an IP host via the dial plan mapper. The IP host has a direct connection to either the destination telephone number or a PBX.
5. The session application then runs the H.323 session protocol to establish a transmission and a reception channel for each direction over the IP network. If the call is being handled by a PBX, the PBX forwards the call to the destination telephone. If RSVP has been configured, the RSVP reservations are put into effect to achieve the desired quality of service over the IP network.
6. The CODECs are enabled for both ends of the connection and the conversation proceeds using RTP/UDP/IP as the protocol stack.
7. When either end of the call hangs up, the RSVP reservations are torn down (if RSVP is used) and the session ends. Each end becomes idle, waiting for the next off-hook condition to trigger another call setup.

### 9.15.3 Prerequisite Tasks

Before you can configure your D-LinkIP telephone equipments to use Voice over IP, you must first:

- Establish a working IP network.
- Install the voice network module and the voice card into D-Link router (Voice port of V100 is fixed).
- Complete your company's dial plan.
- Establish a working telephony network based on your company's dial plan.
- Integrate your dial plan and telephony network into your existing IP network topology. Merging your IP and telephony networks depends on your particular IP and telephony network topology. In general, we recommend the following suggestions: Use canonical numbers wherever possible. It is important to avoid situations where numbering systems are significantly different on different routers or access servers in your network.

- Make routing and/or dialing transparent to the user—for example, avoid secondary dial tones from secondary switches, where possible.
- Contact your PBX vendor for instructions about how to reconfigure the appropriate PBX interfaces.
- After you have analyzed your dial plan and decided how to integrate it into your existing IP network, you are ready to configure your network devices to support Voice over IP.

#### 9.15.4 Voice over IP Configuration Task List

To configure VoIP on D-Link IP phone receiver, you should complete the configuration of Dial Peers.

At first use command `dial-peer terminator` in global configuration mode. There's no terminator configuration by default. Dial mode is that once the user presses key it matches the called number. User can use this command to configure '#' or '\*' to be terminator. Thus the called number is matched only when the user input terminator.

Use the **dial-peer** command to define dial peers and switch to the dial-peer configuration mode. Each dial peer defines the characteristics associated with a call leg. A call leg is a discrete segment of a call connection that lies between two points in the connection. An end-to-end call is comprised of four call legs, two from the perspective of the source access server, and two from the perspective of the destination access server. Dial peers are used to apply attributes to call legs and to identify call origin and destination. There are two different kinds of dial peers:

**POTS**—Dial peer describing the characteristics of a traditional telephony network connection. POTS peers point to a particular voice port on a voice network device. To minimally configure a POTS dial peer, you need to configure the following two characteristics: associated telephone number and logical interface. Use the **destination-pattern** command to associate a telephone number with a POTS peer. Use the **port** command to associate a specific logical interface with a POTS peers.

**VoIP**—Dial peer describing the characteristics of a packet network connection; in the case of Voice over IP, this is an IP network. VoIP peers point to specific VoIP devices. To minimally configure a VoIP peer, you need to configure the following two characteristics: associated destination telephone number and a destination IP address. Use the **destination-pattern** command to define the destination telephone number associated with a VoIP peer. Use the **session** command to specify a destination IP address for a VoIP peer.

##### Note:

- The binding phone numbers of any two dial peers can't be the same, because it will result that one number is mapped to multiple ports (POTS) or multiple IP address (VoIP), thereby at loose ends.
- If dial-peer terminator hasn't been configured in global configuration mode, then the dial matching method is overlapped, namely that number is matched once the user presses key. Thus a phone number A binded by a dial peer is the prefix of another phone number B, and it will result that B is expected to be dialed and A is actually dialed.

Multiple phone numbers (POTS) can be bound on a port and multiple phone number (VoIP) can be bound on an IP address. In fact, the illegal configurations that list above can not be implemented by using command.

Refer to the chapter "[Configure Dial Peer](#)" to get some additional information about dial-peer and dialing.

#### 9.15.5 Configure Dial Peers

The key point to understand how Voice over IP functions is to understand dial peers. Each dial peer defines the characteristics associated with a call leg, as shown in Figure 1 and Figure 2. A call leg is a discrete segment of a call connection that lies between two points in the connection. All the call legs for a particular connection have the same connection ID.

Four call legs make comprise and end-to-end call—two from the perspective of the source router as shown in Figure 1, and two from the perspective of the destination router as shown in Figure 2. Dial peers are used to apply attributes to call legs and to identify call origin and destination.

Dial peers are used for both inbound and outbound call legs. An inbound call leg originates outside the router. An

outbound call leg originates from the router. For inbound call legs, a POTS dial peer might be associated to the calling setup. POTS peers associate a telephone number with a particular voice port so that incoming calls for that telephone number can be received and outgoing calls can be placed. For outbound call legs, this call is associated with the the VoIP dial peer at setup time. VoIP peers associate destination telephone numbers with a specific IP address so that outgoing calls can be placed.

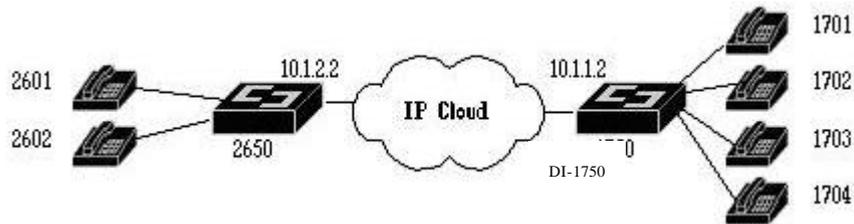


Figure 3 IP Voice Equipment Connection

To configure call connectivity between the source and destination as illustrated in Figure 3, enter the following commands on 2650 (10.1.2.2):

```
2650_config#dial-peer voice 1 pots
2650_config_dialpeer#destination pattern 2601
2650_config_dialpeer#port 1/0
2650_config_dialpeer#exit
2650_config#dial-peer voice 2 pots
2650_config_dialpeer#destination pattern 2602
2650_config_dialpeer#port 1/1
2650_config_dialpeer#exit
2650_config#dial-peer voice 3 voip
2650_config_dialpeer#destination-pattern 170.
2650_config_dialpeer#session target ipv4: 10.1.1.2
2650_config_dialpeer#exit
```

enter the following commands on 1750(10.1.1.2):

```
1750_config#dial-peer voice 1 pots
1750_config_dialpeer#destination-pattern 1701
1750_config_dialpeer#port 1/0
1750_config_dialpeer#exit
1750_config#dial-peer voice 2 pots
1750_config_dialpeer#destination-pattern 1702
1750_config_dialpeer#port 1/1
1750_config_dialpeer#exit
1750_config#dial-peer voice 3 pots
1750_config_dialpeer#destination-pattern 1703
1750_config_dialpeer#port 2/0
1750_config_dialpeer#exit
1750_config#dial-peer voice 4 pots
1750_config_dialpeer#destination-pattern 1704
1750_config_dialpeer#port 2/1
1750_config_dialpeer#exit
1750_config#dial-peer voice 5 voip
1750_config_dialpeer#destination-pattern 260.
1750_config_dialpeer#session target ipv4: 10.1.2.2
1750_config_dialpeer#exit
```

In the previous configuration example, the last one digits of V100's set-dial-peer 3 was replaced with wildcards “.”. This

means that from 2650(10.1.2.2), calling any number string that begins with the digits "176" will result in a connection to 1750 router (10.1.1.2). This implies that 1750 router (10.1.1.2) services all numbers beginning with those digits and follow a digit behind.

The **shutdown** and **codec** command did not use in the previous configuration example, please see the “Correlative Voice Command”.

### 9.15.6 Create a Dial Peer Configuration Table

There is specific data relative to each dial peer that needs to be identified before you can configure dial peers in Voice over IP. One way to do this is to create a peer configuration table.

Using the example in Figure 4, 1750 router (inserted two dual-port FXS voice cards) with an IP address of 10.1.1.2, connects a small sales branch office to the main office through 3660 router (inserted one dual-port FXS voice card) with an IP address of 10.1.2.2. There are four telephones in the sales branch office that need to be established as dial peers. 3660 router is the primary gateway to the main office; as such, it needs to be connected to the company's PBX. There are four devices that need to be established as dial peers in the main office, all of which are basic telephones connected to the PBX.

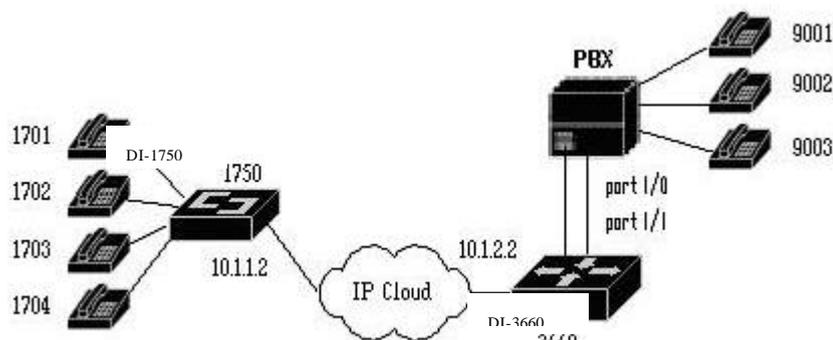


Figure 4 VoIP Voice Network Example

Following table is the peer configuration table for the example illustrated in Figure 4.

| Dial Peer | Number | Types | Voice Port | Target IP Address |
|-----------|--------|-------|------------|-------------------|
| 1750      |        |       |            |                   |
| 1         | 1761   | POTS  | 1/0        |                   |
| 2         | 1762   | POTS  | 1/1        |                   |
| 3         | 1763   | POTS  | 2/0        |                   |
| 4         | 1764   | POTS  | 2/1        |                   |
| 10        | 900.   | VoIP  |            | 10.1.2.2          |
| 3660      |        |       |            |                   |
| 1         | 176 .  | VoIP  |            | 10.1.1.2          |
| 2         | 900.   | POTS  | 1/0 和 1/1  |                   |

### 9.15.7 Configure POTS Dial Peers

To configure a POTS peer, you need to define its telephone number(s), and associate it with a voice port through which calls will be established. To enter the dial-peer configuration mode and select POTS as the method of voice-related encapsulation, use the following command in global configuration mode:

| Command | Sub-command and arguments | Function |
|---------|---------------------------|----------|
|---------|---------------------------|----------|

|                  |                              |                                                                                                                                                       |
|------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dial-peer</b> | <b>voice <i>num</i> pots</b> | Enter the dial-peer configuration mode to configure a POTS peer. The <i>num</i> value of the command is a tag that uniquely identifies the dial peer. |
|------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|

To configure the identified POTS peer, use the following commands in dial-peer configuration mode:

| Step | Command                    | Sub-command and parameters | Function                                                                                                                                                                                                                                                                                       |
|------|----------------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>destination-pattern</b> | <i>STR</i> [T]             | Define the phone number concerned with POTS dial-peer.                                                                                                                                                                                                                                         |
| 2    | <b>port</b>                | <i>slot/port</i>           | Associate the special voice port with POTS dial-peer.                                                                                                                                                                                                                                          |
| 3    | <b>trim_prefix</b>         | <i>number</i>              | This command has different meaning in different course.<br>In POTS peers, if local called port is FXO port, the process will peel off the first few numbers automatically and dial left numbers to PBX automatically. Refer to the presentation of VOIP peers below for meaning of VOIP peers. |

### 9.15.8 Configure VoIP Dial Peers

To configure a VoIP peer, you need to uniquely identify the peer (by assigning it a unique tag number), define its destination telephone number and destination IP address. To enter the dial-peer configuration mode, use the following command in global configuration mode:

| Command          | Sub-command and parameters   | Function                                                                                                                                                                      |
|------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dial-peer</b> | <b>voice <i>num</i> voip</b> | Enter the dial-peer configuration mode to configure a VoIP peer. The <i>number</i> value of the dial-peer voice voip command is a tag that uniquely identifies the dial peer. |

To configure the identified VoIP peer, use the following commands in dial-peer configuration mode:

| Step | Command                    | Sub-command and parameters                                      | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|----------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>destination-pattern</b> | <i>STR</i> [T]                                                  | Define the destination telephone number associated with this VoIP dial peer. The <i>string</i> argument is telephone number with the length less than 15, which include the wildcard “.”                                                                                                                                                                                                                                                                      |
| 2    | <b>Session</b>             | <b>target { ipv4:<br/><i>ip_addr</i>  <br/>terminal   ras }</b> | <i>Destination-address</i> specifies destination IP address for the dial peer.<br><b>Terminal</b> indicates that the set-dial-peer is used to call H.323 terminal device such as Microsoft Netmeeting. Here the <b>config-destination-pattern</b> command is used to mark the IP address of H.323 terminal device. The format likes A.B.C.D. After dots are taken out, 0 is padded in each field less than 3-bit. If the <b>config-trim-prefix</b> command is |

|   |                    |                   |                                                                                                                                                                                                                                                                                                                                                                        |
|---|--------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |                    |                   | configured, get rid of the appointed prefix and examine IP address according upper rule.<br><b>Ras</b> indicates that the destination address information bound by the set-dial-peer can be got through RAS dynamic parsing.                                                                                                                                           |
| 3 | <b>codec</b>       | <i>codec_type</i> | Configure all the codec for the dialog.                                                                                                                                                                                                                                                                                                                                |
| 4 | <b>trim_prefix</b> | <i>number</i>     | This command has different meanings in different course. In VOIP dial-peer, this command is meaningful when <b>session terminal</b> is configured. And the meaning is that the first few numbers input by user will be peeled off and the left numbers will be examined into destination IP address. The meanings of POTS dial-peers are shown in upper presentations. |
| 5 | <b>require-qos</b> |                   | This indicates that the communication of the dial-peer needs the QoS guarantee.                                                                                                                                                                                                                                                                                        |

*codec\_type*: {g711ar64 | g711ur64 | g729r8 | g729-compatible | g723r53 | g723r63 | g726r32 | g726r40 | g727r32 | g727r40 }

### Configure the replace of VoIP dial-peer

As configuring dial-peer, you can configure replace dial-peer so that you can use the replace dial-peer which has specified ID to process dialing when you can't dial through using dial-peer.

| Command            | Sub-command and parameters | Function                                                 |
|--------------------|----------------------------|----------------------------------------------------------|
| <b>alternative</b> | <i>num preference num</i>  | Configure the replace dial-peer as well as its priority. |

After configuring this function, when failing in dialing, it will use the replace dial-peer in turn of priority to make dialing until succeeding in dialing or failing in dialing all replace dial-peer. The replace of replace dial-peer won't be used in current dialing.

### 9.16 Validation Tips

You can check the validity of your dial-peer configuration by performing the following tasks:

If you have relatively few dial peers configured, you can use the **show run** command to verify that the data configured is correct. Use this command to display a specific dial peer or to display all configured dial peers.

### 9.17 Troubleshooting Tips

If you are having trouble connecting a call and you suspect the problem is associated with dial-peer configuration, you can try to resolve the problem by performing the following tasks:

- As to FXS port, if the off hook of connected phone hasn't dialling tone, please examine whether POTS dial-peer has been configured for the FXS port.
- Check whether the VoIP dialling is relevant to the binding phone number and the IP address.
- Ping the associated IP address to confirm connectivity.
- To verify that the IP phone receiver have been configured correctly, use **show run** command on the local and remote IP phone receivers.
- Use debug commands such as **debug vpm**, **debug h323**, **debug H225**, **debug H245**.

### Configure voice port

At present D-Link voice ports have three types: FXS, FXO and E&M. Their configure commands are different from each other. Normally it is enough of using port default configuration. Refer to IP voice command index for detailed specification.

To change voice port configuration, please use the following command in global configure mode:

| Command           | Sub-command and parameters | Function                                                                                                                                                     |
|-------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>voice-port</b> | <i>slot/port</i>           | Enter into voice port configure mode to configure corresponding voice port. <i>slot</i> is the slot number the port residing on. <i>port</i> is port number. |

### 通用配置 Command

here 列出一些常用配置 Command :

| Command                | Sub-command and parameters | Function                                                                                                                                                        |
|------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>comfort-noise</b>   |                            | Specify whether to output background noise as silent voice occurring between the both sides.                                                                    |
| <b>connection-plar</b> | <i>STR</i>                 | After receiving the hanging up of the other side on voice port, it will evoke a VOIP call by the port according to the hot line dialing configured on the port. |
| <b>description</b>     | <i>STR</i>                 | Add specification on specified voice port so that the configurator won't be confused as operating.                                                              |
| <b>output-gain</b>     | <i>NUM</i>                 | Configure the volume played to the user on voice port.                                                                                                          |
| <b>Shutdown</b>        |                            | Disable the current voice port.                                                                                                                                 |

### E&M port special configure

Considering different configuration of different PBX products, we show you about the usual configure commands when configuring E&M port.

| Command             | Sub-command and parameters                   | Function                                                                                                              |
|---------------------|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>operation</b>    | <i>{2-wire / 4-wire }</i>                    |                                                                                                                       |
| <b>emsignal-in</b>  | <i>{immediate / wink-start / delay-dial}</i> | Configure the wire connected with voice port using the signal adopted by E&M port as the switch calling current port. |
| <b>emsignal-out</b> | <i>{immediate / wink-start / delay-dial}</i> | Configure the signal adopted on E&M port as the current port calling the switch.                                      |
| <b>type</b>         | <i>{1 / 2 / 3 / 5}</i>                       | Configure the connecting type of the voice port.                                                                      |

### FXO port special configure

As using FXO port you should first examine the switch frequency and accommodate it.

As using FXO port you are usually needed to sense the switch frequency and tune the frequency. (Refer to "About DSP sensing switch signaling tone" for detailed specification.)

| Command      | Sub-command and parameters                                                                             | Function                                                                                                                                                                                                                                                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>sense</b> | <b>cptone port</b> <i>slot/port</i><br><b>dial</b> [ <i>STR</i> ] <i>tone_type</i><br><i>freq_type</i> | This command is used to sense the frequency and wave type of various signaling tone of the switch connected directly or indirectly with FXO port on the router. Through configuring different dial_string and processing corresponding operating (similar as common phone) when sensing, you can sense various signaling tones on different switches. |

|               |             |                                                                                           |
|---------------|-------------|-------------------------------------------------------------------------------------------|
| <b>cptone</b> | <i>slot</i> | Configure the parameters of a slot, here all the ports on the slot must be in IDLE state. |
|---------------|-------------|-------------------------------------------------------------------------------------------|

( Note: Command sense is used in global mode.

### 9.17.1 Voice over IP Configuration Examples

The actual Voice over IP configuration procedure you complete depends on the actual topology of your voice network. The following configuration examples should give you a starting point. Of course, these configuration examples would need to be customized to reflect your network topology.

Configuration procedures are supplied for the following scenarios:

- FXS-to-FXS Connection
- PSTN Gateway Access Using FXO Connection

These examples are described in the following sections.

**Note :** Each machine must be configured the IP address used by the voice gateway at one time.

Such as in example 1, configuration of 1750\_1 is as below:

```
1750_1_config#gateway-cfg
1750_1_config_gw#gateway ipaddr 10.1.1.1
```

### 9.17.2 FXS-to-FXS Connection

In this example, a very small company, consisting of two offices, has decided to integrate Voice over IP into its existing IP network. One basic telephony device is connected to V100\_1; therefore V100\_1 has been configured for two POTS peers and one VoIP peer. Because two telephony devices are connected to V100\_2, it has also been configured for two POTS peers and one VoIP peer. Figure 5 illustrates the topology of this FXS-to-FXS connection example.

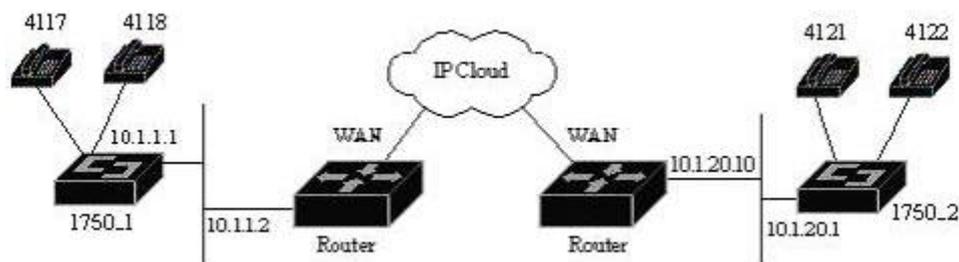


Figure 5 FXS-to-FXS Connection Example

```
1750_1 configuration
1750_1_config#interface e1/0
1750_1_config_e1/0#ip address 10.1.1.1 255.255.255.0
1750_1_config_e1/0#exit
1750_1_config#ip route default 10.1.1.2
1750_1_config#dial-peer voice 1 pots
1750_1_config_dialpeer#destination-pattern 4117
1750_1_config_dialpeer#port 0/0
1750_1_config_dialpeer#exit
1750_1_config#dial-peer voice 2 pots
1750_1_config_dialpeer#destination-pattern 4118
1750_1_config_dialpeer#port 0/1
1750_1_config_dialpeer#exit
```

```

1750_1_config#dial-peer voice 3 voip
1750_1_config_dialpeer#session target 10.1.20.1
1750_1_config_dialpeer#destination-pattern 412.
1750_1_config_dialpeer#exit
1750_1_config#wr
1750_2 configuration
1750_2_config#interface e1/0
1750_2_config_e1/0#ip address 10.1.20.1 255.255.255.0
1750_2_config_e1/0#exit
1750_2_config#ip route default 10.1.20.10
1750_2_config#dial-peer voice 1 pots
1750_2_config_dialpeer#destination-pattern 4121
1750_2_config_dialpeer#port 0/0
1750_2_config_dialpeer#exit
1750_2_config#dial-peer voice 2 pots
1750_2_config_dialpeer#destination-pattern 4122
1750_2_config_dialpeer#port 0/1
1750_2_config_dialpeer#exit
1750_2_config#dial-peer voice 3 voip
1750_2_config_dialpeer#session target 10.1.1.1
1750_2_config_dialpeer#destination-pattern 411.
1750_2_config_dialpeer#exit
1750_2_config#wr

```

### 9.17.3 PSTN Gateway Access Using FXO Connection

The following example shows how to configure Voice over IP to link users with the PSTN gateway using an FXO connection. In this example, users connected to 2650 in Shanghai can reach PSTN users in Beijing. Router 1750 in Beijing is connected directly to the PSTN through an FXO interface. Suppose that the length of telephone number on PSTN in Beijing is 8 bits. The call code of Beijing is 010. 2560 in Shanghai uses FXS port to connect with telephone. Router 1750 in Beijing uses FXO port to connect with telephone port on PSTN. Suppose the port number on PSTN is A. Then users in Shanghai can use the phone, whose number is 8011 (8012), to call directly any phone in Beijing. And to call 8011 (8012), PSTN users in Beijing must first dial number A and dial 8011 (8012) after two dialing tones. Figure 6 illustrates the topology of this connection example.

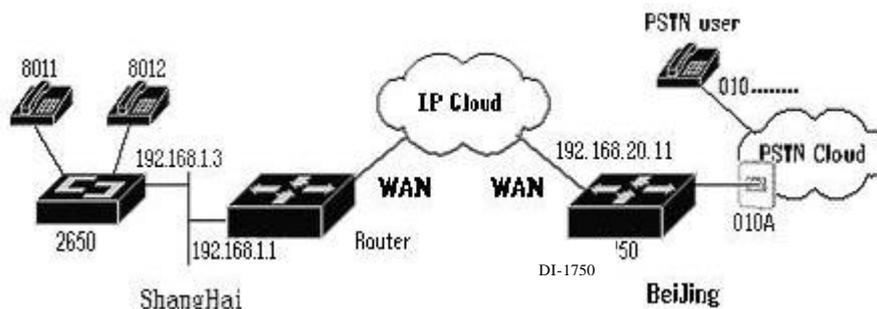


Figure 6 PSTN Gateway Access Using FXO Connection Example

Note:

**This example assumes that the company already has established a working IP connection between its two remote offices.**

```

2650 configuration
2650_config#interface e1/0

```

```

2650_config_e1/0#ip address 192.168.1.3 255.255.255.0
2650_config_e1/0#exit
2650_config#ip route default 192.168.1.1
2650_config#dial-peer voice 1 pots
2650_config_dialpeer#destination-pattern 8011
2650_config_dialpeer#port 1/0
2650_config_dialpeer#exit
2650_config#dial-peer voice 2 pots
2650_config_dialpeer#destination-pattern 8012
2650_config_dialpeer#port 0/1
2650_config_dialpeer#exit
2650_config #dial-peer voice 10 voip
2650_config_dialpeer#session target 192.168.20.11
2650_config_dialpeer#destination-pattern 010.....
2650_config_dialpeer#exit
2650_config#wr
1750 dial peer configuration
1750_config#dial-peer voice 1 pots
1750_config_dialpeer#port 1/0
1750_config_dialpeer#destination-pattern 010.....
1750_config_dialpeer#exit
1750_config#dial-peer voice 2 voip
1750_config_dialpeer#session target 192.168.1.3
1750_config_dialpeer#destination-pattern 8011
1750_config_dialpeer#exit
1750_config#dial-peer voice 3 voip
1750_config_dialpeer#session target 192.168.1.3
1750_config_dialpeer#destination-pattern 8012
1750_config_dialpeer#exit
1750_config#wr

```

### Use IP connection to connect two FXO

In some cases, it is very useful of using IP network to connect two PBX. The following example demonstrates how to configure voice over IP so that it can use IP connection and FXO port to connect up different PSTN. Generally PBX uses pattern 5, 4 wire, outputs signal immediate and input signal delay-dial. This example is configured according this mode and uses the pattern of establishing call through GK. 3660\_3 acts as GK.

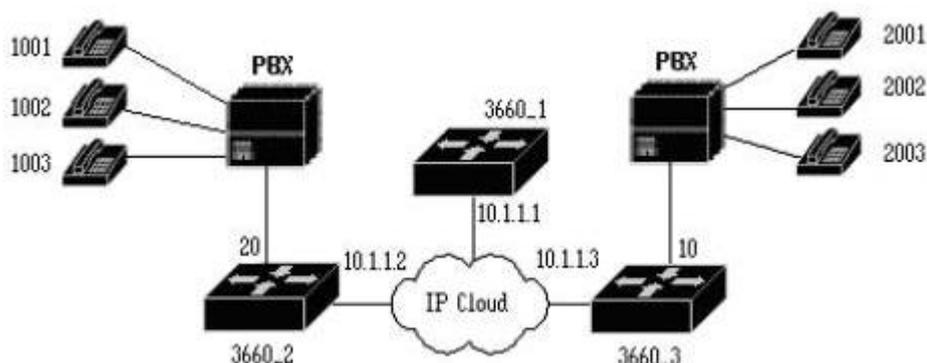


Figure 7 – IP connection between FXOs

```

3660_1 configure :
3660_1_config#inter e1/0
3660_1_config_e1/0#ip address 10.1.1.1 255.255.255.0
3660_1_config_e1/0#exit

```

```
3660_1_config#gatekeeper
3660_1_config_gatekeeper#zone local gkbdcom bdcom.com interface Ethernet0/0
3660_1_config_gatekeeper#gw-type-prefix 20.... gw ipaddr 10.1.1.2
3660_1_config_gatekeeper#gw-type-prefix 10.... gw ipaddr 10.1.1.3
3660_1_config_gatekeeper#no shutdown
3660_1_config_gatekeeper#exit
3660_1_config#
```

3660\_2 configure :

```
3660_2_config#inter e1/0
3660_2_config_e1/0#ip address 10.1.1.2 255.255.255.0
3660_2_config_e1/0#exit
3660_2_config_dial-peer voice 1 pots
3660_2_config_dialpeer#destination-partten 200000
3660_2_config_dialpeer#port 1/0
3660_2_config_dialpeer#exit
3660_2_config_dial-peer voice 2 pots
3660_2_config_dialpeer#destination-partten 20....
3660_2_config_dialpeer#port 1/0
3660_2_config_dialpeer#trim-prefix 2
3660_2_config_dialpeer#exit
3660_2_config_dial-peer voice 3 voip
3660_2_config_dialpeer#destination-partten 10....
3660_2_config_dialpeer#session target ras
3660_2_config_dialpeer#exit
3660_2_config_gateway
3660_2_config_gateway#gateway ipaddr 10.1.1.2
3660_2_config_gateway#gateway gkid gkbdcom bdcom.com ipaddr 10.1.1.1
3660_2_config_gateway#no shutdown
3660_2_config#
```

3660\_3 configure :

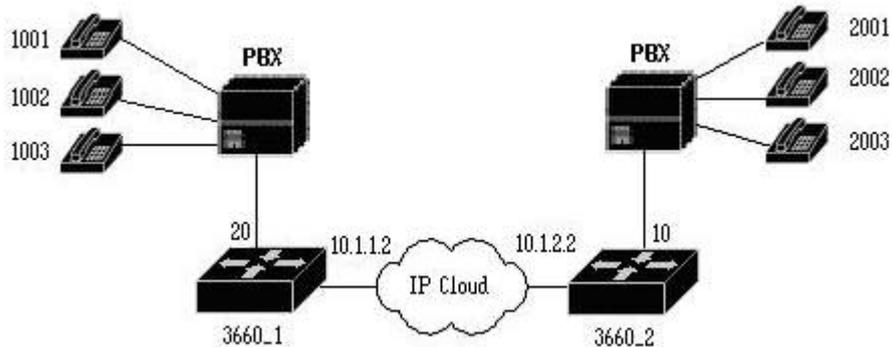
```
3660_3_config#inter e1/0
3660_3_config_e1/0#ip address 10.1.1.3 255.255.255.0
3660_3_config_e1/0#exit
3660_3_config_dial-peer voice 1 pots
3660_3_config_dialpeer#destination-partten 100000
3660_3_config_dialpeer#port 1/0
3660_3_config_dialpeer#exit
3660_3_config_dial-peer voice 2 pots
3660_3_config_dialpeer#destination-partten 10....
3660_3_config_dialpeer#port 1/0
3660_3_config_dialpeer#trim-prefix 2
3660_3_config_dialpeer#exit
3660_3_config_dial-peer voice 3 voip
3660_3_config_dialpeer#destination-partten 20....
3660_3_config_dialpeer#session target ras
3660_3_config_dialpeer#exit
3660_3_config_gateway
3660_3_config_gateway#gateway ipaddr 10.1.1.3
3660_3_config_gateway#gateway gkid gkbdcom bdcom.com ipaddr 10.1.1.1
```

```
3660_3_config_gateway#no shutdown
3660_3_config#
```

### Configuration in using E&M connection

The following example demonstrates how to configure Voice over IP so that it can use E&M port to connect up different PSTNs.

Common PBX uses pattern 5, 4 wire, outputs immediate and inputs signal delay-dial. This example is configured according to this mode.



**Figure 8 – Remote connection between E&Ms**

3660\_1 configure :

```
3660_1_config#inter e1/0
3660_1_config_e1/0#inter e1/0
3660_1_config_e1/0#ip address 10.1.1.2 255.255.255.0
3660_1_config_e1/0#exit
3660_1_config#voice-port 1/0
3660_1_config_voiceport#type 5
3660_1_config_voiceport#operation 4-wire
3660_1_config_voiceport#emsignal-in immediate
3660_1_config_voiceport#emsignal-out delay-dial
3660_1_config_voiceport#exit
3660_1_config#dial-peer voice 1 pots
3660_1_config_dialpeer#destination-partten 20
3660_1_config_dialpeer#port 1/0
3660_1_config_dialpeer#exit
3660_1_config#dial-peer voice 2 voip
3660_1_config_dialpeer#destination-partten 10...
3660_1_config_dialpeer#session target ipv4: 10.1.2.2
3660_1_config_dialpeer#exit
3660_1_config#
```

3660\_2 configure :

```
3660_2_config#inter e1/0
3660_2_config_e1/0#inter e1/0
3660_2_config_e1/0#ip address 10.1.1.2 255.255.255.0
3660_2_config_e1/0#exit
3660_2_config#voice-port 1/0
3660_2_config_voiceport#type 5
3660_2_config_voiceport#operation 4-wire
3660_2_config_voiceport#emsignal-in immediate
3660_2_config_voiceport#emsignal-out delay-dial
3660_2_config_voiceport#exit
3660_2_config#dial-peer voice 1 pots
```

```

3660_2_config_dialpeer#destination-partten 10
3660_2_config_dialpeer#port 1/0
3660_2_config_dialpeer#exit
3660_2_config#dial-peer voice 2 voip
3660_2_config_dialpeer#destination-partten 20....
3660_2_config_dialpeer#session target ipv4: 10.1.1.2
3660_2_config_dialpeer#exit
3660_2_config#

```

### Configure dialing replacer

- Layout : Dial 1234 , if failed , configure replace order : 2345 , 3456

Configure command :

```

Router_config#dial-peer voice 10 voip
Router_config_dialpeer#destination 1234
Router_config_dialpeer#session target ras
Router_config_dialpeer#alternative 20 preference 0
Router_config_dialpeer#alternative 21 preference 2
Router_config_dialpeer#ex
Router_config#dial-peer voice 20 voip
Router_config_dialpeer#destination 2345
Router_config_dialpeer#session target ras
Router_config_dialpeer#ex
Router_config#dial-peer voice 21 voip
Router_config_dialpeer#destination 3456
Router_config_dialpeer#session target ras
Router_config_dialpeer#ex

```

You can use dialpeers with the same number to be replacer, but as configuring, you must arrange the primary dialpeer in the front and the replaced dialpeer in the behind. (You can use command **show running** to examine it.) Because it is processed in turn of arrangement and according to the rule of first matching first using when processing dialing query. So we suggest you first configure primary dialpeer and then configure replacing dialpeer, or in layout configure the replacing dialpeer ID to be larger than primary dialpeer and use the command in global configure mode to align dialpeers by ID.

**Note :**

- **The phone number configured in dialpeer used by replacer must be available number, viz. there is no dot or letter T.**

**Command aline-dialpeer is non-resumable, please use it after perfect layout.**

Configure the fax function based on Voice over IP

The way of configuring is to configure fax-protocol t38/rtp in dialpeer of voip. It will employ bypass mode to processing fax while there is not the two commands.

Our voice products now support two fax mode: T38 and RTP. The fax rate only supports default value 14400pbs. The fax configuration of FXS and FXO is consistent.

### BYPASS Fax

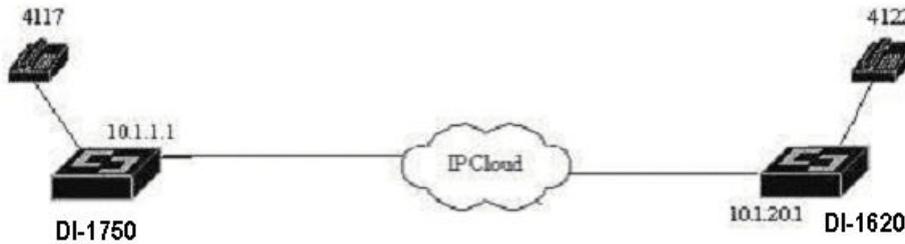
This is the default mode of D-Link router. It is the recommended mode if you have enough bandwidth. At present, as our device specifies codec to be g711ar64, g711ur64, g726r32, dg726r40, g727r32 and g727r40, you can use bypass to fax. PCM coding is a lossless coding mode, therefore the fax signal is best in this coding mode and certainly this fax occupies the most bandwidth. We suggest you configure codec to be g711ar64 or g711ur64 when taking this fax mode.

### T38 Fax

This fax mode is the most saving mode as to bandwidth. We support faxing with versions more advanced than cisco12.2.x IOS. When cisco device has been configured with fax protocol t38, we can communicate with it correctly.

What you should care is that the high speed redundancy and low speed redundancy of our current T38 are both 0 (default value). So when you process t38 fax communicating with Cisco router, its high speed redundancy and low speed redundancy must also be 0 (default value). In addition, the two voice codings g729r8 and g729-compatible don't support t38 fax.

For an example, BDCOM1750 and Cisco2620 is processing t38 fax , as demonstrated in the following figure :



DI-1750 configure :

```

1750_config#interface e1/0
1750_config_e1/0#ip address 10.1.1.1 255.255.255.0
1750_config_e1/0#exit
1750_config#dial-peer voice 1 pots
1750_config_dialpeer#destination-pattern 4117
1750_config_dialpeer#port 1/0
1750_config_dialpeer#exit
1750_config#dial-peer voice 2 voip
1750_config_dialpeer#session target ipv4:10.1.20.1
1750_config_dialpeer#destination-pattern 4122
1750_config_dialpeer#codec g723r53
1750_config_dialpeer#fax t38
1750_config_dialpeer#exit
1750_config#write
  
```

DI-2620 configure :

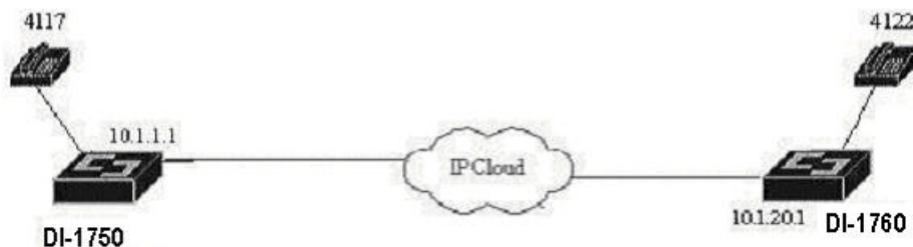
```

2620_config#interface e0/0
2620_config_e0/0#ip address 10.1.20.1 255.255.255.0
2620_config_e0/0#exit
2620_config#dial-peer voice 1 pots
2620_config_dialpeer#destination-pattern 4122
2620_config_dialpeer#port 1/0
2620_config_dialpeer#exit
2620_config#dial-peer voice 2 voip
2620_config_dialpeer#session target ipv4:10.1.1.1
2620_config_dialpeer#destination-pattern 4117
2620_config_dialpeer#codec g723r53
2620_config_dialpeer#fax protocol t38
2620_config_dialpeer#exit
2620_config#write
  
```

## RTP Fax

We support RTP faxing with Huawei devices. As configuring you should care that the D-Link router only needs to configure fax rtp mode while Huawei router should be configured in fax protocol t38 mode, and in Huawei router you should also configure fax rate 14400 and fax train-mode ppp, as t38 fax in Huawei router is actually transferred in RTP mode. In addition, g729r8 and g729-compatible don't support rtp fax.

For an example, in the following figure BDCOM1750 is processing rtp faxing with Huawei1760:



DI-1750-1 configure :

```
1750_config#interface e1/0
1750_config_e1/0#ip address 10.1.1.1 255.255.255.0
1750_config_e1/0#exit
1750_config#dial-peer voice 1 pots
1750_config_dialpeer#destination-pattern 4117
1750_config_dialpeer#port 1/0
1750_config_dialpeer#exit
1750_config#dial-peer voice 2 voip
1750_config_dialpeer#session target ipv4:10.1.20.1
1750_config_dialpeer#destination-pattern 4122
1750_config_dialpeer#codec g723r53
1750_config_dialpeer#fax rtp
1750_config_dialpeer#exit
1750_config#write
```

DI-1760 configure :

```
1760_config#interface e0/0
1760_config_e0/0#ip address 10.1.20.1 255.255.255.0
1760_config_e0/0#exit
1760_config#dial-peer voice 1 pots
1760_config_dialpeer#destination-pattern 4122
1760_config_dialpeer#port 1/0
1760_config_dialpeer#exit
1760_config#dial-peer voice 2 voip
1760_config_dialpeer#session target ipv4:10.1.1.1
1760_config_dialpeer#destination-pattern 4117
1760_config_dialpeer#codec g723r53
1760_config_dialpeer#fax protocol t38
1760_config_dialpeer#fax rate 14400
1760_config_dialpeer#fax train-mode ppp
1760_config_dialpeer#exit
1760_config#write
```

### Configure Gateway and Gatekeeper of Voice over IP

Our VoIP Gateway primarily supplies accessing of PSTN and IP network, supplies proper translation between transmitting form (such as from/to H.225.0 to/from H.221) and communicating program in order to transparently reflect the character from a network point to as SCN point or inverted. VoIP Gatekeeper primarily supplies the management function of gateway, including register managing, bandwidth managing, accessing managing, area managing and calling managing and so on. It is optional in H.323 system.

In this chapter we will mainly introduce the following content:

- Configure voice gateway
- Configure voice gatekeeper

- Example of voice gateway and gatekeeper configuration

### Configure Voice over IP gateway

This section will specify how to configure VoIP gateway on an IP phone.

#### Configure gateway

To configure voice gateway, you should enter into voice gateway configure mode and use the following command in global configure mode:

| Command            | Sub-command and parameters | Function                                              |
|--------------------|----------------------------|-------------------------------------------------------|
| <b>gateway-cfg</b> |                            | Enter into voice gateway configure mode to configure. |

The basic step of voice gateway configure is as below:

| Step | Command        | Sub-command and parameters                                   | Function                                                                                                                                                                                              |
|------|----------------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>gateway</b> | <b>ipaddr</b> <i>ipaddr</i>                                  | Configure the address used by gateway, thereinto ipaddr must be an existing local address. (Support virtual address)                                                                                  |
| 2    |                | <b>gkid</b> <i>gkname</i> <b>ipaddr</b> <i>ipaddr [port]</i> | Configure the gatekeeper registered by gateway. If port has not been configured, it will use the default port 1719. The default port is recommended (It must be identical with port configure on GK.) |
| 3    |                | <b>h323id</b> <i>string</i>                                  | Configure H.323 ID used by gateway. This ID will be registered on gatekeeper. If it uses domain name form, then the name suffix must be identical with domain name configured on GK.                  |
| 4    |                | <b>tech-prefix</b> <i>string</i>                             | Configure the technique prefix registered on gatekeeper. It can be multiple and is up to 8.                                                                                                           |

**Note :** Command **gateway tech-prefix** is invalide to the device registered to D-Link GK , because the command **gw-type-prefix D-Link** currently supported is defined differently with Cisco. This command will be valid to device registered to Cisco GK.

#### Examine tips

You can examine your voice gateway configuration through excuting the following tasks:

- Use command **show gateway** to show voice gateway configure state.
- Use command **show running** to show voice gateway configure content.

#### Troubleshooting tips

If you are having trouble connecting a call and you suspect the problem is associated with gateway configuration, you can try to resolve the problem by performing the following tasks:

- Examine IP address and gatekeeper of the gateway.
- Use the command **show getekway** to confirm the voice gateway on the devices have been properly configured.
- Use these debug commands: **debug voip event asn**, **debug voip event ras**, **debug voip event gw**.

### Configure Voice over IP Gatekeeper

This section will show you how to configure VoIP gatekeeper.

#### Configure gatekeeper

To configure voice gatekeeper, you should enter into voice gatekeeper configure mode and use the following command in global configure mode:

| Command               | Sub-command and parameters | Function                                           |
|-----------------------|----------------------------|----------------------------------------------------|
| <b>gatekeeper-cfg</b> |                            | Enter into gatekeeper configure mode to configure. |

The basic configuration of voice gatekeeper is as below:

| Step | Command     | Sub-command and parameters                       | Function                                                                                                                   |
|------|-------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1    | <b>zone</b> | <b>local</b> <i>gkname domain ipaddr</i>         | Configure the local domain information , <i>ipaddr</i> must be an existing local address.                                  |
| 2    |             | <b>remote</b> <i>gkname domain ipaddr [port]</i> | Configure remote domain information. If port is not configured it will used the default port. Default port is recommended. |
| 3    |             | <b>prefix</b> <i>gkname string</i>               | Configure domain prefix.                                                                                                   |

### Examine tips

You can perform the following tasks to examine your gatekeeper configuration:

- Use command **show gatekeeper** to show gatekeeper state.
- Use command **show running** to show gatekeeper content.

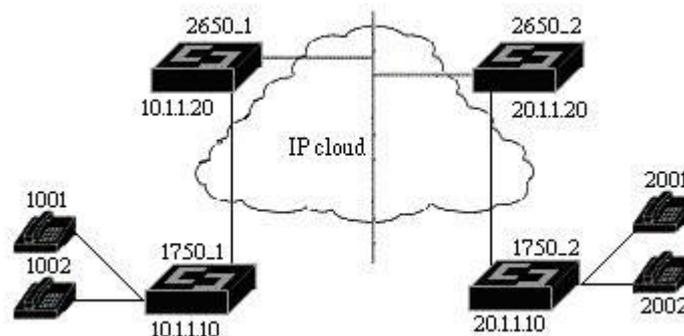
### Troubleshooting tips

If you are having trouble connecting a call and you suspect the problem is associated with gatekeeper configuration, you can try to resolve the problem by performing the following tasks:

- Examine gatekeeper IP and information.
- Use command **show gatekeeper** to examine that the gatekeeper have been properly configured on these devices.
- Use debug command **debug voip event asn**, **debug voip event ras**, **debug voip event gw**.

### Example of VoIP gateway and gatekeeper configure

Demonstrated in the following figure is two 1750 gateway respectively registered to two 2650 gatekeeper.



**Figure 9 – Connecting between gateway and gatekeeper**

2650\_1 configure:

```
2650_config#interface e1/0
2650_config_e1/0#ip address 10.1.1.20 255.255.255.0
2650_config_e1/0#exit
2650_1_config#gatekeeper-cfg
2650_1_config_gk#zone local gk1 zone1.com 10.1.1.20
2650_1_config_gk#zone remote gk2 zone2.com 20.1.1.20
2650_1_config_gk#zone prefix gk2 20..
2650_1_config_gk#exit
```

```

2650_1_config#wr
1750_1 configure:
2650_config#interface e1/0
2650_config_e1/0#ip address 10.1.1.10 255.255.255.0
2650_config_e1/0#exit
1750_1_config#gateway-cfg
1750_1_config_gw#gateway ipaddr 10.1.1.10
1750_1_config_gw#gateway gkid gk1 ipaddr 10.1.1.20
1750_1_config_gw#gateway h323id 10@zone1.com
1750_1_config_gw#exit
1750_1_config#wr
2650_2 configure:
2650_config#interface e1/0
2650_config_e1/0#ip address 20.1.1.20 255.255.255.0
2650_config_e1/0#exit
2650_2_config#gatekeeper-cfg
2650_2_config_gk#zone local gk2 zone2.com 20.1.1.20
2650_2_config_gk#zone remote gk1 zone1.com 10.1.1.20
2650_2_config_gk#zone prefix gk1 10..
2650_2_config_gk#exit
2650_2_config#wr
1750_2 configure:
2650_config#interface e1/0
2650_config_e1/0#ip address 20.1.1.10 255.255.255.0
2650_config_e1/0#exit
1750_2_config#gateway-cfg
1750_2_config_gw#gateway ipaddr 20.1.1.10
1750_2_config_gw#gateway gkid gk1 ipaddr 20.1.1.20
1750_2_config_gw#gateway h323id 10@zone2.com
1750_2_config_gw#exit
1750_2_config#wr

```

## Configure IVR

IVR is a function module in D-Link voice product and takes charge of voice exchanging and supports voice authentic cost service. Its cost function needs cooperate of RADIUS server. If you select RADIUS in authentication, you should also configure RADIUS server. This chapter mainly produces some basic IVR configuration.

As processing AAA operating on IP voice call and even logging specification of each call, you should get the identity of the caller. This information (caller identity) is either the caller number or a number/password peer pre-configured. In the second case, the IP phone user needs to input a set of numbers before inputing number/password peer, in order to inform the IP phone system the following step is to input number/password peer (Otherwise the system will consider number/password peer to be called number and process parsing.) This set of numbers is what we called access service number.

In fact the user taking caller number to be authenticator can also use access service number, which may be a consideration of uniform costing (A group of users use one access service number.) or be a convenience for maintenance of call purview. Therefore we have three dial flows (The first is called one dial flow and the last two called two dial flow.).

- Directly dial the called number.
- First dial access service number and then dial the called number.

- First dial access service number, then input number/password peer and finally input called number.

Voice RADIUS can supply the upper three different basic access flow according to user configuring and configure the flow parameters (such as re-dial times, number/password and so on).

To mask all IVR configuration one-off, we supply a general switch for throughout IVR service function. Shut down this switch, all IVR will stop functioning. It is enabled by default. Please perform the following configuration in ivr configure mode:

| Command    | Sub-command and parameters         | Function            |
|------------|------------------------------------|---------------------|
| <b>ivr</b> | { <b>enable</b>   <b>disable</b> } | Enable/Disable IVR. |

Default configuration is *enable*.

We will introduce the following contents to you:

- Configure access number
- Configure dial flow as well as concerned parameters
- Configure ivr phone
- Configure direct ivr authentication mode
- Configure one-off ivr dial mode
- Configure ivr record mode
- Enable RADIUS authentication
- Enable RADIUS costing

### Configure access number

As to a two-dial user, he must first dial a special access number then he could achieve IP phone service. So you must configure corresponding access number before enable two-dial service.

Please perform the following configuring in dial-peer ivr configure mode:

| Command                    | Sub-command and parameters | Function                     |
|----------------------------|----------------------------|------------------------------|
| <b>destination-pattern</b> | <i>des-num</i>             | Configure ivr access number. |

### Configure dial flow as well as concerned parameters

#### 9.18 Configure dial flow

Access number essentially is only a symbol of dial flow. You must configure a series of parameters for it in order to implement a real dial flow. Although each parameter has default value, it can support the basic service without configuring.

Two-dial can be divided into two flows: Caller flow (caller authentication) and card number flow (card number/password authentication). So you must specify the dial flow to each access number.

### Configure ivr card phone

#### 9.18.1 Configuration in IVR dial-peer

To configure a card phone, you are needed to first configure pattern name and ivr access number in dial-peer configure mode. Please perform the following configurations in dial-peer configure mode:

| Command                    | Sub-command and parameters | Function                               |
|----------------------------|----------------------------|----------------------------------------|
| <b>destination-pattern</b> | <i>des-num</i>             | Configure ivr access number.           |
| <b>app</b>                 | <i>ivrl_card</i>           | Specify the ivr pattern is card phone. |

You can configure card number length and password length only after you have configured card phone. As to the times of re-authenticating after failing, this configuration will also affect the authentication times of direct authentication.

What is needed to avoid is that the user doesn't input phone number for a long time. The period from user inputting first key to factually pressing first key is called first dial time. The period from user pressing first key to the end of the whole dial process is called whole dial time. Here you can configure the wait time of user first dial time and the wait time of user whole dial time. When user exceeded this time, his card number would also be considered to be invalid.

### 9.18.2 Configure authentication information

You can configure authentication account information, configure card number length, password length and re-authenticating times. The length of card number and password dose not include ending key. You can also configure the wait time of authentication, first dial and whole dial process.

Please perform the following configuration in ivr configure mode:

| Command       | Sub-command and parameters                | Function                                                                                 |
|---------------|-------------------------------------------|------------------------------------------------------------------------------------------|
| <b>authen</b> | <b>card</b> <i>card-len key-len times</i> | Configure card number length, password length and re-authentication times on card phone. |
|               | <b>time-out</b> <i>time1 time2</i>        | Configure the wait time of first dial and whole dial.                                    |

The first parameter of first command is default card number length, he second parameter is default password length and the third parameter is re-authentication times. The first parameter of second command is the wait time of first dial, the second parameter is the wait time of whole dial. In default case card number length is 10, password length is 10 and re-authentication times is 3.

### 9.18.3 Configure dial information

You can configure the length of called phone number, wait time of first dial and whole time. The period from user starting dial to actually press key is called first dial wait time. The period from user first pressing to ending dial is called whole dial wait time.

As to the phone number length, you can dial ending key (default key is "#")for end when the called number has not enough length. But if your called number length is larger than the configured length, it won't continue dialing after the configured length and the dial will end.

You can configure the wait time of first dial and whole dial. What you should care is that this command will take effect on dial length and wait time of all patterns. Please perform the following configuration in ivr configure mode:

| Command     | Sub-command and parameters                | Function                                                        |
|-------------|-------------------------------------------|-----------------------------------------------------------------|
| <b>dial</b> | <b>dialing</b> <i>numlen dialing-time</i> | Configure the length of called number and the times of re-dial. |
|             | <b>timeout</b> <i>time1 time2</i>         | Configure the wait time of first dial and whole dial.           |

The first parameter of the first command is default phone number length and the second parameter is the dialing times allowed in a dial process. The first parameter of the second command is the wait time of first dial and the second parameter is the wait time of whole dial. In default case the length of phone number is 10 and the dialing times is 3.

### Configure the balance prompt tone and the cost rate

You will care the balance on your card as using card phone, thus there is a problem of balance query. But you may be bored by the whiny balance prompt, then you can use balance prompt switch. Please perform the following configuration in ivr configure mode:

| Command              | Sub-command and parameters | Function                        |
|----------------------|----------------------------|---------------------------------|
| <b>account-audio</b> |                            | Configure voice balance prompt. |

No *account-audio* is configured by default.

Configure the money amount corresponding to seconds in the relevant server. In fact what stored in the server are all the seconds the user can communicate. When offering balance query they are needed to be translated into money. The cast rate is configured for the translation. Please perform the following configuration in ivr configure mode:

| Command             | Sub-command and parameters | Function                                                             |
|---------------------|----------------------------|----------------------------------------------------------------------|
| <b>account-rate</b> | <i>rate</i>                | Configure the money corresponding to per 6-second. The unit is cent. |

*Cost rate is 3 cents per 6-second.*

Configure ivr direct authentication mode

#### 9.18.4 Configuration in IVR dial-peer

To configure direct authentication mode, you must first configure pattern name and ivr access number in dial-peer configure mode. Please perform the following configuration in dial-peer configure mode:

| Command                    | Sub-command and parameters | Function                                                    |
|----------------------------|----------------------------|-------------------------------------------------------------|
| <b>destination-pattern</b> | <i>des-num</i>             | Configure ivr access number.                                |
| <b>app</b>                 | <i>ivr_direct_authen</i>   | Configure the ivr pattern to be direct authentication mode. |

#### Configure dial information

You can configure the length of called number, the wait time of first dial and whole dial. The length of called number doesn't include ending key.

The period from user starting dial to actually press key is called first dial wait time. The period from user first pressing to ending dial is called whole dial wait time. You can configure the wait time of first dial and whole dial. What you should care is that this command will take effect on dial length and wait time of all patterns. Please perform the following configuration in ivr configure mode:

Please perform the following configuration in ivr configure mode:

| Command     | Sub-command and parameters                | Function                                                          |
|-------------|-------------------------------------------|-------------------------------------------------------------------|
| <b>dial</b> | <b>dialing</b> <i>numlen dialing-time</i> | Configure the default called number length and the re-dial times. |
|             | <b>timeout</b> <i>time1 time2</i>         | Configure the wait time of first dial and whole dial.             |

*In default case: numlen = 10, dialing-time = 3, dial timeout time1 = 30 seconds, time2 = 60 seconds*

#### Configure ivr one-dial mode

If you enable one-dial mode, it won't enable single authentication to a special user, so it can only execute uniform authenticating to all one-dial users.

To configure one-dial mode, you are only needed to configure gw-authen-h323Command in global configure mode.

Please perform the following configuration in global mode:

| Command               | Sub-command and parameters | Function                        |
|-----------------------|----------------------------|---------------------------------|
| <b>gw-authen-h323</b> |                            | Enable one-dial authentication. |

*There's no this switch by default.*

Configure ivr record mode

### 9.18.5 Configuration in IVR dial-peer

To configure record mode, you should first configure pattern name and ivr access number in dial-peer configure mode. Please perform the following configurations in dial-peer ivr configure mode:

| Command                    | Sub-command and parameters | Function                                       |
|----------------------------|----------------------------|------------------------------------------------|
| <b>destination-pattern</b> | <i>des-num</i>             | Configure ivr access number.                   |
| <b>app</b>                 | <i>ivrl_record</i>         | Configure record function of this ivr pattern. |

As to record you are needed to configure some parameters. At first you should configure the aim file name of the record, thus the record file can be achieved. Default file name is "user". As to the file recorded by the user himself, after the rebooting the the router, it will record some child files and these file names are increase from "1".

For an example, given a file name is "user", then the first record file will be "user/1", the second will be "user/2", and so on.

### 9.18.7 Configure record file name

Please perform the following configuration in ivr configure mode:

| Command     | Sub-command and parameters                   | Function                        |
|-------------|----------------------------------------------|---------------------------------|
| <b>file</b> | <b>record-gather-name</b><br><i>filename</i> | Configure the record file name. |

The parameter is the string of record file name. It is "user" by default.

After having configured the aim record file name you will care the time of once recording. We have supplied the default once recording time and you can precise it into seconds or 0.1 second in which the record will be more perfect.

### 9.18.6 Configure the default recording time

We offered time parameters in two different units, but they are both the once recording time. In the two parameters the minimum will take effect, and in default they are 300 (s) and 100 (0.1s). Please perform the following configuration in ivr configure mode:

| Command       | Sub-command and parameters     | Function                             |
|---------------|--------------------------------|--------------------------------------|
| <b>record</b> | <b>time</b> <i>time1 time2</i> | Configure default time of recording. |

The first parameter and the second parameter are all default once recording time. But the unit of first parameter is second, but the second is 0.1 sendond. The default once recording time is 15-second.

#### For an example:

```
record time 12 10
```

It indicates the default recording time is 12-second and  $10 * 0.1 = 1$  second, then the time 1 second will take effect.

### Configure the playing position of the file

After completing recording, you should set the record file to the specified position so that you can get the sound. Then we will show you this process. Given a user has got a sound file named "user/1" according to the upper steps, then he can set the file to the specified position and make it be the sounde file used in ivr voice pattern. It will take the D-Link sound by default.

You can configure the file name of welcome word for card phone, the prompt sound of inputing user name, the prompt sound of inputing password, the prompt sound of failing in authentication, the prompt sound file name of starting dialing phone number, the prompt sound file name of failing in getting through the call, the prompt sound file name of balance not enough. Please perform the following configurations in ivr configure mode:

| Command | Sub-command and parameters               | Function                                                               |
|---------|------------------------------------------|------------------------------------------------------------------------|
| file    | <b>play-start</b> <i>filename</i>        | Configure the file name of welcome word on card phone.                 |
|         | <b>authen-user-start</b> <i>filename</i> | Configure the prompt sound of inputing user name.                      |
|         | <b>authen-key-start</b> <i>filename</i>  | Configure the prompt sound of inputing password.                       |
|         | <b>authen-failed</b> <i>filename</i>     | Configure the prompt sound file name of failing in authentication.     |
|         | <b>dial-start</b> <i>filename</i>        | Configure the prompt sound file name of starting dialing phone number. |
|         | <b>dial-failed</b> <i>filename</i>       | Configure the prompt file name of failing in putting through the call. |
|         | <b>interrupt-start</b> <i>filename</i>   | Configure the prompt sound file name of balance no enough.             |

### Enable RADIUS authentication

If you enable one-dial mode, it won't enable single authentication to a special user, so it can only execute uniform authenticating to all one-dial users.

You should also ensure the interconnection between RADIUS Server and RADIUS Client in network layer, and ensure in the RADIUS Server you have configured the user list of all one-dial users. No authentication is enabled by default.

Please perform the following configuration in global mode:

| Command               | Sub-command and parameters | Function                                   |
|-----------------------|----------------------------|--------------------------------------------|
| <b>gw-authen-h323</b> |                            | Enable or disable one-dial authentication. |

The authentication function to two-dial user is fixed in the pattern and can't be changed.

### Enable RADIUS costing

Although the authentication function is separated between one-dial user and two-dial user, the costing function is the same. When you enable this function on a RADIUS Client, the system will evoke costing to all one-dial and two-dial users and send the information to specified RADIUS Server for costing. RADIUS costing is disabled by default. Please perform the following configuration in global mode:

| Command                   | Sub-command and parameters | Function                                         |
|---------------------------|----------------------------|--------------------------------------------------|
| <b>gw-accounting-h323</b> |                            | Enable or disable costing function to all users. |

#### Configure the method of sending RADIUS costing information:

There's no default method for the costing request corresponding from RADIUS Client to RADIUS. Please perform the following configuration in global mode:

| Command    | Sub-command and parameters                                                     | Function                                             |
|------------|--------------------------------------------------------------------------------|------------------------------------------------------|
| <b>aaa</b> | <b>accounting connection h323</b> {none   wait-start   stop_only   start_stop} | Configure the method of sending costing information. |

### Examine Tips

You can examine your ivr configuration through the following task:

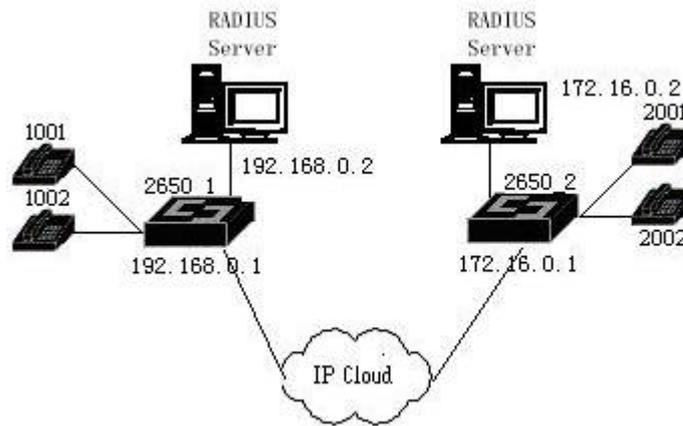
- Use Command **show voip ivr configuration** to show relevant ivr configuration.

### Troubleshooting Tips

If there's some trouble in using ivr voice exchanging or costing authentication, you can complete the following tasks to resolve the problems:

- Examine **radius** configuration , Examine **aaa** configuration.
- Use command **show voip ivr configuration** to examine ivr configuration on these devices.
- Use command **show voip ivr ivri-session**、 **show voip ivr call-instance** to show the running instructure information.
- Use command **debug voip event ivri**、 **debug voip event ivrc**、 **debug voip event ivrp** for debug.

### Examples of IVR costing authentication



**Figure 10 – IVR authentication costing configuration**

Example 1- configuration of different ivr pattern

2650\_1 configuration

```

2650_1_config#dial-peer voice 10 pots
2650_1_config_dialpeer #des 1001
2650_1_config_dialpeer #exit
2650_1_config#dial-peer voice 11 pots
2650_1_config_dialpeer #des 1002
2650_1_config_dialpeer #exit
2650_config#aaa authentication login def radius
2650_config#aaa accounting connection h323 wait-start radius
2650_config#interface e1/0
2650_config_e1/0#ip address 192.168.0.1 255.255.255.0
2650_config_e1/0#exit
2650_1_config#gw-accounting-h323
2650_1_config#gw-authen-h323
2650_1_config#radius server 192.168.0.2
2650_1_config#radius key 1111
2650_1_config#dial-peer voice 01 ivr
2650_1_config_dialpeer#des 101
2650_1_config_dialpeer#application ivrl_card
2650_1_config_dialpeer#exit
2650_1_config#dial-peer voice 02 ivr
2650_1_config_dialpeer#des 102
2650_1_config_dialpeer#application ivrl_direct_authen
2650_1_config_dialpeer#exit
2650_1_config#dial-peer voice 03 ivr
2650_1_config_dialpeer#des 103
2650_1_config_dialpeer#application ivrl_record

```

```
2650_1_config_dialpeer#exit
2650_1_config#wr

2650_1_config#ivr-cfg
2650_1_config_ivr#account-audio
2650_1_config_ivr#default account-audio
2650_1_config_ivr#account-rate 4
2650_1_config_ivr#default account-rate
2650_1_config_ivr#authen card 6 7 3
2650_1_config_ivr#authen timeout 10 20
2650_1_config_ivr#default default authen
2650_1_config_ivr#dial dialing 6 4
2650_1_config_ivr#dial timeout 40 50
2650_1_config_ivr#default dial
2650_1_config_ivr#file record-gather-name user2
2650_1_config_ivr#file play-start user/1
2650_1_config_ivr#file record-start user/2
2650_1_config_ivr#file record-again user/3
2650_1_config_ivr#file record-failed user/4
2650_1_config_ivr#file authen-user-start user/5
2650_1_config_ivr#file authen-key-start user/6
2650_1_config_ivr#file authen-failed user/7
2650_1_config_ivr#file dial-start user/8
2650_1_config_ivr#file dial-failed user/9
2650_1_config_ivr#file interrupt-start user/10
2650_1_config_ivr#def file
2650_1_config_ivr#record time 5 34
2650_1_config_ivr#record key * 1
2650_1_config_ivr#default record
2650_1_config_ivr#stop-key *
2650_1_config_ivr#default stop-key
2650_1_config#wr
```

#### Example 2 - Card phon configuration

```
2650_1_config#dial-peer voice 10 pots
2650_1_config_dialpeer #des 1001
2650_1_config_dialpeer #exit
2650_1_config#dial-peer voice 11 pots
2650_1_config_dialpeer#des 1002
2650_1_config_dialpeer#exit
2650_config#aaa authentication login def radius
2650_config#aaa accounting connection h323 wait-start radius
2650_config#interface e1/0
2650_config_e1/0#ip address 192.168.0.1 255.255.255.0
2650_config_e1/0#exit
2650_1_config#gw-accounting-h323
2650_1_config#radius server 192.168.0.2
2650_1_config#radius key 1111
2650_1_config#dial-peer voice 01 ivr
```

```
2650_1_config_dialpeer#des 101
```

```
2650_1_config_dialpeer#app ivrl_card
```

```
2650_1_config_dialpeer#exit
```

```
2650_1_config# ivr-cfg
```

```
2650_1_config_ivr#account_audio
```

```
2650_1_config_ivr#exit
```

```
2650_1_config#wr
```

#### Example 3 - Direct authentication configuration

```
2650_1_config#dial-peer voice 10 pots
```

```
2650_1_config_dialpeer #des 1001
```

```
2650_1_config_dialpeer #exit
```

```
2650_1_config#dial-peer voice 11 pots
```

```
2650_1_config_dialpeer#des 1002
```

```
2650_1_config_dialpeer#exit
```

```
2650_config#aaa authentication login def radius
```

```
2650_config#aaa accounting connection h323 wait-start radius
```

```
2650_config#interface e1/0
```

```
2650_config_e1/0#ip address 192.168.0.1 255.255.255.0
```

```
2650_config_e1/0#exit
```

```
2650_1_config#gw-accounting-h323
```

```
2650_1_config#radius server 192.168.0.2
```

```
2650_1_config#radius key 1111
```

```
2650_1_config#dial-peer voice 01 ivr
```

```
2650_1_config_dialpeer#des 101
```

```
2650_1_config_dialpeer#app ivrl_direct_authen
```

```
2650_1_config_dialpeer#exit
```

```
2650_1_config#wr
```

#### Example 4 - once authentication configuration

```
2650_1_config#dial-peer voice 10 pots
```

```
2650_1_config_dialpeer #des 1001
```

```
2650_1_config_dialpeer #exit
```

```
2650_1_config#dial-peer voice 11 pots
```

```
2650_1_config_dialpeer#des 1002
```

```
2650_1_config_dialpeer#exit
```

```
2650_config#aaa authentication login def radius
```

```
2650_config#aaa accounting connection h323 wait-start radius
```

```
2650_config#interface e1/0
```

```
2650_config_e1/0#ip address 192.168.0.1 255.255.255.0
```

```
2650_config_e1/0#exit
```

```
2650_1_config#gw-accounting-h323
```

```
2650_1_config#gw-authen-h323
```

```
2650_1_config#radius server 192.168.0.2
```

```
2650_1_config#radius key 1111
```

```
2650_1_config#wr
```

#### Example 5 - Replace the welcome word with record ( in two steps)

Step1 :

```
2650_1_config#dial-peer voice 10 pots
2650_1_config_dialpeer #des 1001
2650_1_config_dialpeer #exit
2650_1_config#dial-peer voice 11 pots
```

## 10. IBM Networking Configuration

### 10.1 Configure DLSW Task List

#### 10.1.1 Configure DLSW

Before configuring DLSW, you should first get some knowledge of DLSW, which is helpful. Data Link Switching is a new protocol of channel or encapsulation. It can encapsulate the frames from Logical Link Control Type1 or Type2 of SNA and NetBIOS system, and make it get across non-SNA network. DLSw resolved the limitation that LLC2 designed based on LAN can ' t transmit in WAN. DLSw offers a series of solutions for the transition of SNA networks to TCP/IP networks.

DLSw is designed to replace the former various channel protocol that established by multiple network developers. While developing the DLSW module, the developers considered the IBM large computer and its proprietary SNA network structure system that widely applied by Bank system. DLSW module will follow the international standard of DLSW and compatible with CISCO router DLSw+.

#### 10.1.2 How to use DLSw Configuration Commands

You can process DLSw debug with the offered configuration commands, including DLSw local configuration, DLSw remote configuration, DLSw reachable and unreachable resource configuration, static MAC address configuration and the DLSw bridge group configuration. This will function largely to your DLSw testing.

Configure the following commands in global configuration state:

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dlsw local - peer</b> [peer-id <i>ip-address</i> ] [cost <i>cost</i> ] [if <i>size</i> ] [keepalive <i>seconds</i> ] [init-pacing-window <i>size</i> ] [max-pacing-window <i>size</i> ] [promiscuous]                                                                                                                                                                                                                                     | This command is used to configure the DLSw local peer to appoint the local IP address. The no argument is used to cancel the configuration.                                                                         |
| <b>dlsw remote-peer</b> <i>list-number ip-address</i> [backup-peer <i>ip-address</i> [backup-static   linger <i>minutes</i>   circuit-inactivity <i>minutes</i> ]]   [circuit-weight <i>weight</i> ]   [cost <i>cost</i> ]   [dynamic [inactivity <i>minutes</i>   no-llc <i>minutes</i> ]]   [keepalive <i>seconds</i> ]   [if <i>size</i> ]   [passive]   [priority [priority-vendor-id <i>id-number</i> ]]   [tcp-queue-max <i>size</i> ] | This command is used to configure the remote peer to set up TCP passage. A router can be configured with multiple remote peers. The no argument is used to cancel the configuration.                                |
| <b>dlsw port-list</b> <i>list-number type number</i>                                                                                                                                                                                                                                                                                                                                                                                         | This command is used to configure the port -list, applying the list-number in dlsw remote-peer command, can filter the dlsw message. The no argument is used to cancel the configuration.                           |
| <b>dlsw bgroup-list</b> <i>list-number bgroups number</i>                                                                                                                                                                                                                                                                                                                                                                                    | This command is used to configure the bgroup-list, applying the list-number in remote-peer command, can filter the dlsw message. The no argument is used to cancel the configuration.                               |
| <b>dlsw timer</b> {sna-cache-timeout   explorerer-wait-time} <i>time</i>                                                                                                                                                                                                                                                                                                                                                                     | This command is used to configure the timers used, by now configurable timers are: sna-cache-timeout timer and waiting the response to explorer message clock. The no argument is used to cancel the configuration. |

|                                                                                                                                                                                    |                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dls w load-balance</b> [round-robin   circuit-count<br><i>circuit weight</i> ]                                                                                                  | This command is used to configure the flow-balance from local or remote. The no argument is used to cancel the configuration.                                                          |
| dls w icanreach {mac-exclusive   mac-address<br>mac-addr   saps}                                                                                                                   | This command is used to configure the objects the local dls w can reach. The no argument is used to cancel the configuration.                                                          |
| dls w icannotreach saps sap [sap...]                                                                                                                                               | This command is used to configure the unreachable local SAP. The no argument is used to cancel the configuration.                                                                      |
| dls w mac-addr mac-addr                                                                                                                                                            | This command is used to configure the static MAC address. The no argument is used to cancel the configuration. This command is related to both the local buffer and the remote buffer. |
| dls w bridge-group group-number [sap-priority<br>list-number]                                                                                                                      | This command is used to configure the DLSw bridge group. The no argument is used to cancel the configuration.                                                                          |
| dls w udp-disable                                                                                                                                                                  | This command is used to shut down the UDP sending of dls w. The no argument is used to cancel the configuration.                                                                       |
| <b>sap-priority-list</b> <i>list-number</i><br>[high medium normal low] [dmac <i>mac-address</i> ]<br>[smac <i>mac-address</i> ] [dsap <i>sap-value</i> ] [ssap <i>sap-value</i> ] | This command is used to configure the priority base on MAC/SAP. The no argument is used to cancel the configuration.                                                                   |

### 10.1.3 How to use the function of showing DLSw

Use Commands below in management state and local configuration state:

| Command                                                                              | Purpose                                                                                                                                                  |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| show dls w capabilities [ ip-address<br>ip-address   local ]                         | User can have more understanding about various status which happen during the DLSw capability exchange by displaying the information of DLSw capability. |
| show dls w circuits [detail] [mac-address<br>address   sap-value value   circuit id] | User will know the current status information of all the circuit by displaying DLSw virtue circuit.                                                      |
| show dls w peers [ip-address ip-address ]                                            | By implement this command, it ' ll display the various information about remote DLSw.                                                                    |
| show dls w reachability [[local   remote]  <br>[mac-address address]                 | By implement this command, it'll display the information of DLSw buffer, including the local buffer and remote buffer.                                   |

### 10.1.4 How to use the DLSw's Debug Function

User can use DLSw debug function to monitor the DLSw operation status when using the DLSw function on a router.

User can use the following commands in configuration mode:

| Command                                                                                                                          | Purpose                                             |
|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Debug dlsw error                                                                                                                 | Display debug DLSw error.                           |
| <b>debug dlsw state</b> [ <b>tcp</b> <i>ip-address</i>   <b>circuit</b> <i>circuit-id</i>   <b>explorer</b> <i>mac-address</i> ] | Display debug information of DLSw internal status.  |
| <b>debug dlsw event</b> [ <b>detail</b> ]                                                                                        | Display debug DLSw events                           |
| Debug dlsw flow-control                                                                                                          | Display the debug information of DLSw flow control. |
| Debug dlsw packet                                                                                                                | Display DLSw packet.                                |

### 10.1.5 How to use the DLSw Management Function

User can use the DLSw management function to clear DLSw circuit and statistics when using the DLSw function on a router.

User can use the following command in management mode:

| Command                                         | Purpose               |
|-------------------------------------------------|-----------------------|
| <b>clear dlsw circuit</b> [ <i>circuit-id</i> ] | Clear DLSw circuit    |
| rm dlsw reachability                            | Clear DLSw statistics |

## 10.2 Configuring LLC2

LLC2 (IEEE 802.2) type 2 provides connection-oriented service and is widely used in LAN environments, particularly among IBM communication systems connected by Token Ring. Our router supports LLC2 connections over Ethernet.

LLC2 command provides the function which support the implementation of DLSw protocol.

### LLC2 Configuration Task List

#### 10.2.1 Configure the DLSw idle-time

| Command                       | Purpose                                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| llc2 idle-time <i>seconds</i> | This command is used to control the frequency of polls during periods of idle time (no traffic). Number of seconds (s) that can pass with no traffic before the LLC2 station sends a Receiver Ready frame. The minimum is 1 s. The maximum is 60s, default value is 10 s. |
| llc2 (undo) idle-time         | Return to the default value                                                                                                                                                                                                                                               |

NOTE: During the idle time, there is no I frame exchanged, sending the RR frame to the remote frequently to ask the remote local be ready to receive the data; Set smaller value can notify the remote in time, while too small may arise much more RR frame sent by network.

Select the LLC2 commands from the interface commands of the global configuration list, all LLC2 selection as follows:

Key Word:

U(undo) D(default) Q(quit)

- (00)ack-max the Max I-frames received before sent acknowledgment
- (01)ack-delay-time the Max time to delay the acknowledgment of I-frames
- (02)holdqueue the max queue lenght
- (03)idle-time the timer for idle
- (04)local-window the local window size
- (05)n2 the retrying counts
- (06)t1-time the timer of receiving an acknowledgment
- (07)tbusy-time the timer of re-querying remote busy
- (08)tpf-time the timer of receive a response PDU(F=1)
- (09)trej-time the timer of receiving a reply to a sent REJ PDU

Please Input the code of command to be excute(0-9): **3**

Input 3 , select <idle-time> item

Key Word:

Q(quit)

(00)<1-60> seconds -- the maximum time for idle

Please Input the code of command to be excute(0-0):**0**

Please input a digital number:**12**

Input 12 , It means sending the RR frame every 12s

Will you excute it? (Y/N):**y**

<![endif]>

### 10.2.2 Configure the wait-for-response time

| Command              | Purpose                                                                                                                                                                                                                                                                                                       |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| llc2 t1-time seconds | This command is used to set the amount of time the router waits for a final response to a poll frame before resending the poll frame.<br>Number of seconds (s) the router waits for a final response to a poll frame before resending the poll frame. The minimum is 1 s. The maximum is 60s. default is 10s. |
| llc2 (undo) t1-time  | Return to default value                                                                                                                                                                                                                                                                                       |

NOTE: The local will wait for the confirmation from the remote after sending I frame every time. If the responding time expires, then send the frame again. Increase the value while operating on lower speed network.

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

U(undo) D(default) Q(quit)

(00)ack-max the Max I-frames received before sent acknowledgment

(01)ack-delay-time the Max time to delay the acknowledgment of I-frames

(02)holdqueue the max queue lenght

(03)idle-time the timer for idle

(04)local-window the local window size

(05)n2 the retrying counts

(06)t1-time the timer of receiving an acknowledgment

(07)tbusy-time the timer of re-querying remote busy

(08)tpf-time the timer of receive a response PDU(F=1)

(09)trej-time the timer of receiving a reply to a sent REJ PDU

Please Input the code of command to be excute(0-9): **6**

<![endif]> Input 6 , select <t1-time> item

Key Word:

Q(quit)

(00)<1-60> seconds -- the time interval for an acknowledgment

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**12**

Input 12 , Setting 12 seconds the waiting time

Will you execute it? (Y/N):y

### 10.2.3 Configure the remote-busy time

| Command                 | Purpose                                                                                                                                                                                                                   |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| llc2 tbusy-time seconds | control the amount of time the router waits until repolling a busy remote station. Number of seconds (s) the router waits before repolling a busy remote station. The minimum is 1 s. The maximum is 60s. default is 10s. |
| llc2 (undo) tbusy-time  | Cancel the configuration                                                                                                                                                                                                  |

NOTE: :An LLC2 station has the ability to tell others that it is temporarily busy, so the other stations will not attempt to send any new information frames. The frames sent to indicate this are called Receiver Not Ready (RNR) frames. Increasing the value will prevent the stations from timing out.

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

U(undo) D(default) Q(quit)

(00)ack-max the Max I-frames received before sent acknowledgment

(01)ack-delay-time the Max time to delay the acknowledgment of I-frames

(02)holdqueue the max queue lenght

(03)idle-time the timer for idle

(04)local-window the local window size

(05)n2 the retrying counts

(06)t1-time the timer of receiving an acknowledgment

(07)tbusy-time the timer of re-querying remote busy

(08)tpf-time the timer of receive a response PDU(F=1)

(09)trej-time the timer of receiving a reply to a sent REJ PDU

Please Input the code of command to be excute(0-9): **7**

<![endif]>Input 7 , select <tbusy-time> item

Key Word:

Q(quit)

(00)<1-60> seconds -- the time interval for an indication of the clearance

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**12**

Input 12 , set the remote-busy time as 12s

Will you excute it? (Y/N):y

<![endif]>

**10.2.4 Configure the response time**

| Command                            | Purpose                                                                                                                                                                                         |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>llc2 tpf-time seconds</code> | This command use for control the remote response time<br>seconds Number of seconds (s) the router waits the response from remote station. The minimum is 1 s. The maximum is 60s. default is 1. |
| <code>llc2 (undo) tpf-time</code>  | Cancel the configuration                                                                                                                                                                        |

NOTE: Sometimes a LLC2 station need to know the status of opposite terminal, so the station will send a command frame that need to response by opposite terminal; The opposite terminal will send back an answer frame while received the command frame. If error occurred, the sending terminal is keeping wait. To avoid this matter, you should start a timer. If the responding time expires, the sending terminal will send another command frame; This command use for set the time of wait for the response command frame from opposite terminal.

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

U(undo) D(default) Q(quit)

(00)ack-max the Max I-frames received before sent acknowledgment

(01)ack-delay-time the Max time to delay the acknowledgment of I-frames

(02)holdqueue the max queue lenght

(03)idle-time the timer for idle

(04)local-window the local window size

(05)n2 the retrying counts

(06)t1-time the timer of receiving an acknowledgment

(07)tbusy-time the timer of re-querying remote busy

(08)tpf-time the timer of receive a response PDU(F=1)

(09)trej-time the timer of receiving a reply to a sent REJ PDU

Please Input the code of command to be excute(0-9): **8**

<![endif]>Input 8 , select <tpf-time> item

Key Word:

Q(quit)

(00)<1-60> seconds -- the time interval for a response PDU(F=1)

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**12**

Input 12 , set the wait peer response time as 12s.

Will you excute it? (Y/N):**y**

**10.2.5 Configure the reject-time**

| Command                             | Purpose                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>llc2 trej-time seconds</code> | This command is used to control the amount of time a router waits for a correct frame after sending a reject (REJ) command to the remote LLC2 station.<br>Number of seconds (s) the router waits for a resend of a rejected frame before sending a reject command to the remote station. The minimum is 1 s. The maximum is 60s.The default value is 3s. |
| <code>llc2 (undo) trej-time</code>  | Cancel the configuration                                                                                                                                                                                                                                                                                                                                 |

NOTE: When an LLC2 station sends an information frame, a sequence number is included in the frame. The LLC2 station that receives these frames will expect to receive them in command. If it does not, it can reject a frame and indicate which frame it is expecting to receive instead. Upon sending a reject, the LLC2 station starts a reject timer. If the frames are not received before this timer expires, the session is disconnected.

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

U(undo) D(default) Q(quit)

(00)ack-max the Max I-frames received before sent acknowledgment

(01)ack-delay-time the Max time to delay the acknowledgment of I-frames

(02)holdqueue the max queue length

(03)idle-time the timer for idle

(04)local-window the local window size

(05)n2 the retrying counts

(06)t1-time the timer of receiving an acknowledgment

(07)tbusy-time the timer of re-querying remote busy

(08)tpf-time the timer of receive a response PDU(F=1)

(09)trej-time the timer of receiving a reply to a sent REJ PDU

Please Input the code of command to be execute(0-9): **9**

<![endif]>Input 9 , select <trej-time> item

Key Word:

Q(quit)

(00)<1-60> seconds -- the time interval for a reply to a sent REJ PDU

Please Input the code of command to be execute(0-0): **0**

Please input a digital number:**12**

Input 12 , set the reject time as 12s

Will you execute it? (Y/N):**y**

### 10.2.6 Configure the LLC2 window size

| Command                        | Purpose                                                                                                                                                                                                                                                                            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| llc2 local-window packet-count | Control the maximum number of information frames the router sends before it waits for an acknowledgment.<br>Maximum number of packets that can be sent before the router must wait for an acknowledgment. The minimum is 1 packet. The maximum is 127 packets. Default value is 7. |
| llc2 (undo) local-window       | Cancel the configuration                                                                                                                                                                                                                                                           |

NOTE: A LLC2-speaking station can send only a predetermined number of frames before it must wait for an acknowledgment from the receiver. Set this number to the maximum value that can be supported by the stations with which the router communicates. Setting this value too large can cause frames to be lost, because the receiving station may not be able to receive all of them.

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

U(undo) D(default) Q(quit)

- (00)ack-max the Max I-frames received before sent acknowledgment
- (01)ack-delay-time the Max time to delay the acknowledgment of I-frames
- (02)holdqueue the max queue length
- (03)idle-time the timer for idle
- (04)local-window the local window size
- (05)n2 the retrying counts
- (06)t1-time the timer of receiving an acknowledgment
- (07)tbusy-time the timer of re-querying remote busy
- (08)tpf-time the timer of receive a response PDU(F=1)
- (09)trej-time the timer of receiving a reply to a sent REJ PDU

Please Input the code of command to be execute(0-9): **4**

<![endif]>input 4 , select <local-windows> item

Key Word:

Q(quit)

(00)<1-127> frames -- Window size

Please Input the code of command to be execute(0-0):**0**

Please input a digital number:**12**

输入 12 , set the window size as 12.

Will you execute it? (Y/N):**y**

### 10.2.7 Configure the holdqueue packet-count

| Command                     | Purpose                                                                                                                                                                                                                                                |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| llc2 holdqueue packet-count | control the maximum local hold packet when the transmission of I frame is forbidden because of the remote-busy.<br>The maximum hold packet of I frame before getting the acknowledge.The maximum is 200 packets, minimum is 20 packets, default is 40. |
| llc2 (undo) holdqueue       | Cancel the configuration                                                                                                                                                                                                                               |

NOTE: A LLC2-speaking station cannot send packets(I frames) when the other end is busy. All the packet should be saved before the receiver clear the busy-state ,however the quantity of the saved packets is limited. This command configure the quantity of these saved packet.

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

U(undo) D(default) Q(quit)

- (00)ack-max the Max I-frames received before sent acknowledgment
- (01)ack-delay-time the Max time to delay the acknowledgment of I-frames
- (02)holdqueue the max queue length
- (03)idle-time the timer for idle
- (04)local-window the local window size
- (05)n2 the retrying counts
- (06)t1-time the timer of receiving an acknowledgment
- (07)tbusy-time the timer of re-querying remote busy
- (08)tpf-time the timer of receive a response PDU(F=1)
- (09)trej-time the timer of receiving a reply to a sent REJ PDU

Please Input the code of command to be execute(0-9): **2**

Input 2 , select <holdqueue> item

Key Word:

Q(quit)

(00)<20-200> number -- queue length

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**120**

Input 120, set the maximum packets as 120 entries

Will you excute it? (Y/N):**y**

### 10.2.8 Configure the ack-delay times(seconds)

When receiving an information frame, a ack frame should be sent. But in order to reduce the unnecessary ack frames, the ACK frames can be delayed. Sending an information frame instead of a ACK frames, if there are information frames sent. If the information frame sent by others have overrun the max size of ACK frames, send a ACK frame immediately not until expire.

| Comman                      | Purpose                    |
|-----------------------------|----------------------------|
| llc2 ack-delay-time seconds | Setting the ACK-delay time |

More details reference the example after

### 10.2.9 Configure the ack-max number

During the ACK-delay times, if the information frames sent by others have been excess the ACK-max number, a ACK frame will be sent immediately to avoid the network-busy misunderstanding by the others. Configuration command as below:

| Command                    | Purpose                    |
|----------------------------|----------------------------|
| llc2 ack-max <i>number</i> | Setting the ACK-max number |

More details reference the example after

### 10.2.10 Show LLC2 link information

| Command                          | Purpose                                                                                                             |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------|
| show llc interface [type number] | This command is used to display the LLC2 link information:<br>type type of the interface<br>number interface number |

NOTE: this command is used to display the LLC2 link status,use the command “show llc” to display the LLC2 link status of the current interface in interface configuration mode.

Input the show command from the interface commands of the global configuration list, it will list all show items, select the IIC, display as fellow:

Key Word:

Q(quit)

(00)interface the llc Tx/Rx and config infomation int interface

(01)<cr>  
 Please Input the code of command to be excute(0-1): 0  
 Input 0  
 Key Word:  
 Q(quit)  
 (00)FastEthernet FastEthernet interface  
 (01)Ethernet Ethernet interface  
 (02)Serial Serial interface  
 (03)Async Asynchronous interface  
 (04)Null Null interface  
 Please Input the code of command to be excute(0-4): 0  
 Input 0 , display the llc2 status of interface f0/0  
 Please input a interface name:f0/0  
 Will you excute it? (Y/N)y  
 Input y , display the information below :

FastEthernet0/0: DOWN  
 ack-time = 12 s, ack-delay-time = 400 ms, idle-time = 12 s  
 pf-time = 12 s, busy-time = 12 s, rej-time = 12 s, N2 = 12  
 IFRAMES 0/0, TESTs 0/0, XIDs 0/0, UIs 0/0  
 FRMRs 0/0, RRs 0/0 RNRs 0/0, REJs 0/0  
 SABMEs 0/0, UAs 0/0, DISCs 0/0, DMs 0/0  
 Discard:0, N(s) err:0, N(r) err:0, Total 0/0

no LLC2 Connections

**10.2.11 Debug the LLC2 link information**

| Command                           | Purpose                                                                                                                                                                                                                                                      |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| debug llc2 [packet][error][state] | This command is mainly used to enable the LLC2 debug.<br>“packet” means enabling the LLC2 data information debugging error ,<br>“error” means enabling the LLC2 error information debugging<br>“state” means enabling the LLC2 status information debugging. |

Select Ilc2 command from management list.

Key Word:  
 Q(quit)  
 (00)errors LLC2 error information  
 (01)packets LLC2 I/O packets  
 (02)state LLC2 state information  
 (03)<cr>  
 Please Input the code of command to be excute(0-3):  
 Input 0 , selecting error parameter  
 Input 1 , selecting packet parameter  
 Input 2 , selecting state parameter

**Example of LLC2 configuration**

You can configure the number of LLC2 frames received before the ACK. In this example, at the time 0, two information frames are received, it doesn't reach the max number 3, so the ACK frames are not sent. If set the 3<sup>rd</sup> ACK frame sent by router can't be received during 800 ms, the delay timer will be active, and then ACK will be sent out.

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

```
U(undo) D(default) Q(quit)
(00)ack-max      the Max I-frames received before sent acknowledgment
(01)ack-delay-time the Max time to delay the acknowledgment of I-frames
(02)holdqueue    the max queue length
(03)idle-time    the timer for idle
(04)local-window the local window size
(05)n2           the retrying counts
(06)t1-time      the timer of receiving an acknowledgment
(07)tbusy-time   the timer of re-querying remote busy
(08)tpf-time     the timer of receive a response PDU(F=1)
(09)trej-time    the timer of receiving a reply to a sent REJ PDU
```

Please Input the code of command to be excute(0-9): **0**

Input 0 , select ack-max item

Key Word:

```
Q(quit)
(00)<1-255> number      -- the Max I-frames received before sent acknowledgme
```

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**3**

Input 3 , setting the max-number of I frame 3

Will you excute it? (Y/N):**y**

Select the IIC2 commands from the interface commands of the global configuration list, all IIC2 selection as follow:

Key Word:

```
U(undo) D(default) Q(quit)
(00)ack-max      the Max I-frames received before sent acknowledgment
(01)ack-delay-time the Max time to delay the acknowledgment of I-frames
(02)holdqueue    the max queue length
(03)idle-time    the timer for idle
(04)local-window the local window size
(05)n2           the retrying counts
(06)t1-time      the timer of receiving an acknowledgment
(07)tbusy-time   the timer of re-querying remote busy
(08)tpf-time     the timer of receive a response PDU(F=1)
(09)trej-time    the timer of receiving a reply to a sent REJ PDU
```

Please Input the code of command to be excute(0-9):**1**

Input 1 , select ack-delay-time item

Key Word:

```
Q(quit)
(00)<10-60000> milliseconds      -- ack-delay-time
```

Please Input the code of command to be excute(0-0): **0**

Please input a digital number:**800**

Input 800 , setting ACK-delay time 800

Will you excute it? (Y/N):**y**

### 10.3 SDLC Configuration Task List

The SDLC tasks described in this section configure the router as an SDLC station. (This is in contrast to a router configured for SDLC Transport, where the device is not an SDLC station, but passes SDLC frames between two SDLC stations across a mixed-media, multiprotocol environment.) The first task is required; you accomplish it with the appropriate set of commands for your network needs. The remaining tasks are optional: you can perform them as necessary to enhance SDLC performance.

#### 10.3.1 Configure the Router as SDLC Primary or Secondary Station

SDLC defines two types of network nodes: primary and secondary. Primary nodes poll secondary nodes in a predetermined order. Secondaries then send if they have outgoing data. When configured as primary and secondary nodes, our devices are established as SDLC stations.

#### 10.3.2 Establishing an SDLC Station for DLSW+ Support

After the router being set as SDLC station, user can use the following commands in interface configuration mode to set the DLSW+ feature:

| Step | Command                                  | Purpose                                                                           |
|------|------------------------------------------|-----------------------------------------------------------------------------------|
| 1    | encapsulation sdlc                       | Set the encapsulation of the serial interface as SDLC.                            |
| 2.   | sdlc role { primary   secondary }        | Set the interface role.                                                           |
| 3.   | sdlc vmac mac-address                    | Set the MAC address of the serial interface                                       |
| 4.   | sdlc partner mac-address<br>sdlc-address | Specify the destination address to set up a inter-connection between SDLC and LLC |

Step 1:

Enter the configuration ports, select 11 item, display:

```
(00)frame-relay Frame Relay Protocol
    (01)hdlc      HDLC Protocol
    (02)ppp      PPP Protocol
    (03)sdlc     SDLC Protocol
    (04)x25     X.25 Protocol
```

Please Input the code of command to be excute(0-4): 3

Input 3 , select sdlc item

Step2:

Select 28 item from listing , display:

```
00)K          The size of the sending window
    .....
    (10)role          SDLC station type
    .....
    Please Input the code of command to be excute(0-16): 10
```

Input 10 item, display:

```
(00)primary          primary station
(01)secondary        secondary station
```

Please Input the code of command to be excute(0-1):

Select interface configuration role

**Step3:**

Select 28 item from listing, display;

```
(00)K          The size of the sending window
.....
(14)vmac      Assign MAC address to interface
.....
Please Input the code of command to be excute(0-16): 14
Input 14 ,select vmac item ,display :
(00)xxxx.xxxx.xxxx      Virtual IEEE MAC address
Please Input the code of command to be excute(0-0): 0
Select 0 , and input mac-address.
```

**Step 4:**

Select 28 item from listing , display:

```
(00)K          The size of the sending window
.....
(06)partner    the remote MAC address for partner
.....
Please Input the code of command to be excute(0-16): 6
Input 6 ,select partner item ,display :
(00)xxxx.xxxx.xxxx Partners Token Ring MAC address
Please Input the code of command to be excute(0-0): 0
Select 0 , and input mac-address , display :
(00)<1-FE>      SDLC Address in Hex
Please Input the code of command to be excute(0-0): 0
Select 0 , and input sdlc-address.
```

The default SDLC role is primary when you want to configure a SDLC multipoint link. The type of physical units which don't has the xid in the SDLC command is PU 21, which is also a default value.

Refer to the chapter “DLSW+ configuration” for more DLSW+ configuration commands.

### 10.3.3 Set the SDLC as Two-way Simultaneous Mode

SDLC two-way simultaneous mode allows a primary SDLC link station to achieve more efficient use of a full-duplex serial line. With two-way simultaneous mode, the primary link station can send data to one secondary link station while there is a poll outstanding. Two-way simultaneous mode works on the SDLC primary side only. On a secondary link station, it responds to a poll from the primary station.

SDLC two-way simultaneous mode operates in either a multidrop link environment or point-to-point link environment.

In a multidrop link environment, a two-way simultaneous primary station is able to poll a secondary station and receive data from the station, and send data (I-frames) to other secondary stations.

In a point-to-point link environment, a two-way simultaneous primary station can send data (I-frames) to the secondary station although there is a poll outstanding, as long as the window limit is not reached.

To configure two-way simultaneous mode, use either of the following commands in interface configuration mode:

| Command                                                               | Purpose                                                                                        |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| sdlc simultaneous full-datamode or<br>sdlc simultaneous half-datamode | Enable the primary station to send data to and receive data from the polled secondary station. |

|  |                                                                                  |
|--|----------------------------------------------------------------------------------|
|  | Prohibit the primary stations from sending data to the polled secondary station. |
|--|----------------------------------------------------------------------------------|

Select 28 item from listing, display:

```
(00)K                The size of the sending window
.....
(13)simultaneous     config the SDLC working in full or half-datamode
.....
Please Input the code of command to be excute(0-16): 13
Input 13 ,select simultaneous item ,display :
(00)full-datamode    full datamode
(01)half-datamode    half datamode
Please Input the code of command to be excute(0-1):
Select the configuration parameters
```

### 10.3.4 Configure SDLC Timer and Retry Counts

When an SDLC station sends a frame, it waits for an acknowledgment from the receiver indicating that this frame has been received. You can modify the time the router allows for an acknowledgment before resending the frame. You can also determine the number of times that a software resends a frame before terminating the SDLC session. By controlling these values, you can reduce network overhead while continuing to check transmission of frames.

To set the SDLC timer and retry counts, use one or both of the following commands in interface configuration mode:

| Command                            | Purpose                                                                          |
|------------------------------------|----------------------------------------------------------------------------------|
| <b>sdlc t1</b> <i>milliseconds</i> | Control the amount of time the software waits for a reply.                       |
| <b>sdlc n2</b> <i>retry-count</i>  | Set the number of times the software will retry an operation that has timed out. |

Take the 1<sup>st</sup> command as an example

Select 28 item from listing, display:

```
(00)K                The size of the sending window
.....
(03)T1              the time of receiving an acknowledgment
.....
Please Input the code of command to be excute(0-16): 3
Input 3 ,select T1 item ,display :
(00)<1-64>           Time to wait for a reply to a frame in seconds
Please Input the code of command to be excute(0-0): 0
Select 0 , and input milliseconds,
```

### 10.3.5 Configure the Amount of SDLC Frames and Information Frames

You can set the maximum size of an incoming frame and set the maximum number of Information-frames (or window size) the router will receive before sending an acknowledgment to the sender. By using higher values, you can reduce network overhead.

To set the amount of SDLC frame and information frame, use any of the following commands in interface configuration mode:

| Command | Purpose |
|---------|---------|
|---------|---------|

|                             |                                                                     |
|-----------------------------|---------------------------------------------------------------------|
| sdlc n1 bit-count           | Set the maximum size of an incoming frame.                          |
| sdlc k window-size          | Set the local window size of the router.                            |
| sdlc poll-limit-value count | Set how many times a primary station will poll a secondary station. |

Take the 1<sup>st</sup> command as an example

Select 28 item from listing, display:

```
(00)K           The size of the sending window
(01)N1         Max number of bytes for incoming frames
(02)N2         Number of retry times
```

.....

Please Input the code of command to be excute(0-16): **1**

Input 1 , select litem , display :

```
(00)<1-1500>      Max number of bytes for incoming frames
```

Please Input the code of command to be excute(0-0): **0**

Select 0 , and input bit-count.

### 10.3.6 Control the Buffer Size

You can control the buffer size on the router. The buffer holds data that is pending transmission to a remote SDLC station. This command is particularly useful in the case of the SDLLC media translator, which allows an LLC2-speaking SNA station on a Token Ring to communicate with an SDLC-speaking SNA station on a serial link. The frame sizes and window sizes on Token Rings are often much larger than those acceptable for serial links, and serial links are often slower than Token Rings.

To control backlogs that can occur during periods of high data transfer from the Token Ring to the serial line, use the following command in interface configuration mode on a per-address basis:

| Command                           | Purpose                                                              |
|-----------------------------------|----------------------------------------------------------------------|
| sdlc holdqueue address queue-size | Set the maximum number of packets held in queue before transmitting. |

Select 28 item from listing, display:

```
(00)K           The size of the sending window
```

.....

```
(05)holdqueue   the max queue length
```

.....

Please Input the code of command to be excute(0-16): **5**

Input 5 , select holdqueue item , display :

```
(00)<1-FE>      SDLC Address in Hex
```

Please Input the code of command to be excute(0-0): **0**

Input 0 , display :

Please input a digital number:Please input a string:

Input address , display :

```
(00)<0-65535>   Queue size
```

Please Input the code of command to be excute(0-0): **0**

Select 0 , and input queue-size.

### 10.3.7 Control Polling of Secondary Stations

You can control the intervals at which the router polls secondary stations, the length of time a primary station can send data to a secondary station, and how often the software polls one secondary station before moving on to the next station.

Keep the following points in mind when using these commands:

- Secondary stations cannot transmit data until they are polled by a primary station. Increasing the poll-pause timer increases the response time of the secondary stations. Decreasing the timer can flood the serial link with unneeded polls, requiring secondary stations to spend wasted CPU time processing them.
- Increasing the value of the poll limit allows for smoother transactions between a primary station and a single secondary station, but can delay polling of other secondary stations.

To control polling of secondary stations, use one or more of the following commands in interface configuration mode:

| Command                            | Purpose                                                                                                                      |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| sdhc poll-pause-timer milliseconds | Set the length of time the router pauses between sending each poll frame to secondary stations on a single serial interface. |
| sdhc poll-limit-value count        | Set how many times a primary station will poll a secondary station.                                                          |

Take the 1<sup>st</sup> command as an example

Select 28 item from listing, display:

```
(00)K                The size of the sending window
.....
(08)poll-pause-timer  the interval of polling the secondary station
.....
Please Input the code of command to be excute(0-16): 8
Input 8 , select poll-pause-timer item , display :
(00)<10-10000>        Time between polls for each secondary SDLC station(ms)
Please Input the code of command to be excute(0-0): 0
Select 0 , and input milliseconds.
```

To retrieve default polling values for these operations, use the **def** forms of these commands.

### 10.3.8 Configure an SDLC Interface for Half-Duplex Mode

By default, SDLC interfaces operate in full-duplex mode. To configure an SDLC interface for half-duplex mode, use the following command in interface configuration mode:

| Command       | Purpose                                           |
|---------------|---------------------------------------------------|
| half-datamode | Configure an SDLC interface for half-duplex mode. |

Select 28 item from listing, display:

```
(00)K                The size of the sending window
.....
(14)simultaneous      config the SDLC working in full or half-datamode
.....
Please Input the code of command to be excute(0-16): 14
Input 14 , select simultaneous item , display :
(00)full-datamode     full datamode
(01)half-datamode     half datamode
Please Input the code of command to be excute(0-16): 1
Input 1 , chose Half-Duplex Mode
```

### Specify the XID Value

The exchange of identification (XID) value you define on the router must match that of the IDBLK and IDNUM system generation parameters defined in VTAM on the Token Ring host to which the SDLC device will be communicating.

NOTE: configuring the XID value will affect the attribute of the interface. If the XID value is configured, it means that the device connected with the interface is PU 2.0. The configuration of XID value must be performed after the interface has been shutdown.

To specify the XID value, use the following command in interface configuration mode:

| Command                           | Purpose                                                       |
|-----------------------------------|---------------------------------------------------------------|
| <code>sdlc xid address xid</code> | Specify the XID value to be associated with the SDLC station. |

Select 28 item from listing, display:

```
(00)K          The size of the sending window
.....
(15)xid        Specify XID value, which determine Pu type
.....
Please Input the code of command to be excute(0-16): 15
Input 15 , select xid item , display :
(00)<1-FE>     SDLC Address in Hex
Please Input the code of command to be excute(0-0): 0
Input 0 , display :
Please input a digital number:Please input a string:
Input address , display :
(00)<1-FFFFFFF>  XID of secondary station in HEX format
Please Input the code of command to be excute(0-0): 0
Select 0 , input xid.
```

<![endif]>

### Set the Largest SDLC Information-Frame Size

Generally, the router and the SDLC device with which it communicates should support the same maximum SDLC I-frame size. The larger this value, the more efficient the line usage, thus increasing performance.

After the SDLC device has been configured to send the largest possible I-frame, you must configure the router to support the same maximum I-frame size. The default is 265 bytes. The maximum value the software can support must be less than the value of the LLC2 largest frame value defined when setting the largest LLC2 I-frame size.

To set the largest SDLC I-frame size, use the following command in interface configuration mode:

| Command                                           | Purpose                                                                                   |
|---------------------------------------------------|-------------------------------------------------------------------------------------------|
| <code>sdlc sdlc-largest-frame address size</code> | Set the largest I-frame size that can be sent or received by the designated SDLC station. |

Select 28 item from listing, display:

```
(00)K          The size of the sending window
.....
(12)sdlc-largest-frame Set max size of received or sent I-frame by station
.....
Please Input the code of command to be excute(0-16): 12
Input 12 , select sdlc-largest-frame item , display :
(00)<1-FE>     SDLC Address in Hex
Please Input the code of command to be excute(0-0): 0
Input 0 , display :
```

Please input a digital number:Please input a string:  
 Input address , display :  
 (00) <0-1500> Largest I-frame size  
 Please Input the code of command to be excute(0-0): **0**  
**Select 0 , and input size.**

### Monitor SDLC Stations

To monitor the configuration of SDLC stations to determine which SDLC parameters need adjustment, use the following command in EXEC mode:

| Command         | Purpose                                         |
|-----------------|-------------------------------------------------|
| show interfaces | Display SDLC station configuration information. |

Input show command , display;

(00)alias alias for command

.....

(19)interface interface status and configuration

.....

Please Input the code of command to be excute(0-47): 19

Input 19 , select interface item , display :

(00)FastEthernet FastEthernet interface

(01)Ethernet Ethernet interface

(02)Serial Serial interface

(03)Async Asynchronous interface

(04)Null Null interface

Please Input the code of command to be excute(0-4): <cr>

Select the configuration interface of the SDLC station to be displayed

### Configuration Examples

The following sections provide SDLC configuration examples:

[SDLC Two-Way Simultaneous Mode Configuration Example](#)

[SDLC Configuration for DLSw+ Example](#)

[Half-Duplex Configuration Example](#)

[sdlc Configuration Example 1-1](#)

[sdlc Configuration Example 1-2](#)

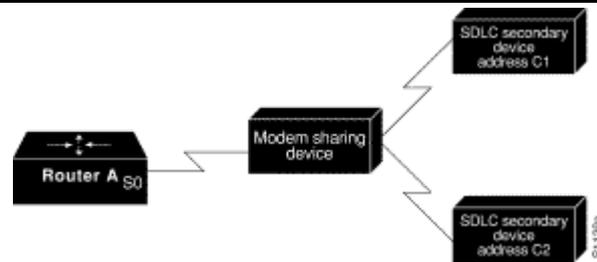
### SDLC Two-Way Simultaneous Mode Configuration Example

The following configuration defines serial interface 0 as the primary SDLC station with two SDLC secondary stations, C1 and C2, attached to it through a modem-sharing device. Two-way simultaneous mode is enabled.

```
config-interface serial 0
  config-encap sdlc -primary
  config-sdlc address c1
  config-sdlc address c2
  sdlc simultaneous full-datamode
```

The network for this configuration is shown in Figure 126.

Figure 126 Two SDLC Secondary Stations Attached to a Single Serial Interface through a Modem-Sharing Device



### SDLC Configuration for DLSw+ Example

The following example describes an SDLC configuration if you plan to implement DLSw+ support. In this example, 4000.3745.0001 is the MAC address of the host. The router serves as the primary station for the remote secondary stations, c1 and c2. Both c1 and c2 are reserved for DLSw+ and cannot be used by any other data link user.

```

config-interface serial 0
  config-encap sdhc
  config-sdhc vmac4000.3174.0000
  config-sdhc address c1
  config-sdhc xid c1 01712345
  config-sdhc partner 4000.3745.0001 c1
  config-sdhc address c2
  config-sdhc xid c2 01767890
  config-sdhc partner 4000.3745.0001 c2
  config-sdhc role primary
  
```

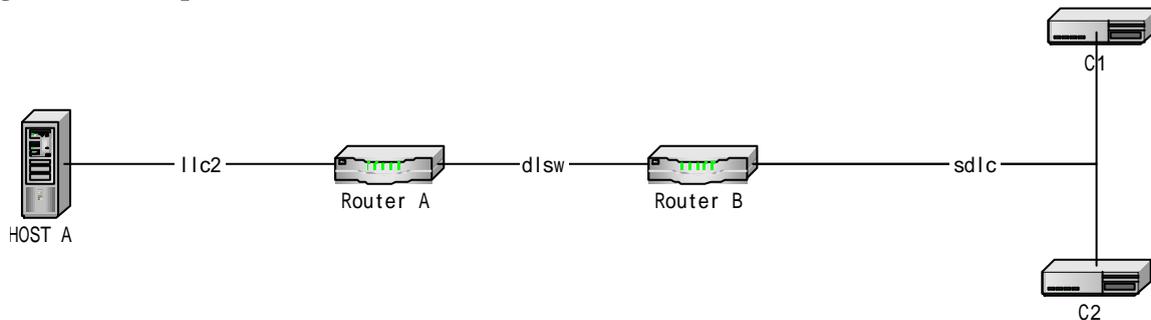
### Half-Duplex Configuration Example

In the following example, an SDLC interface has been configured for half-duplex mode:

```

config-encap sdhc
sdhc simultaneous half-duplex
  
```

### sdhc Configuration Example 1-1



This example describes an SDLC configuration which implements the support for DLSw+. In the example, the MAC address of HOST A is 4000.1111.0001

Router A, as a remote secondary station, is configured as follows:

```

config-interface fastethernet 0
  bridge-group 10
  
```

Router B as remote secondary station: primary station of c1 and c2, c1 and c2 reserved for DLSw+ and can not be used by any other data link user. c1 is PU2.0, c2 is PU2.1. SDLC configuration as below:

```

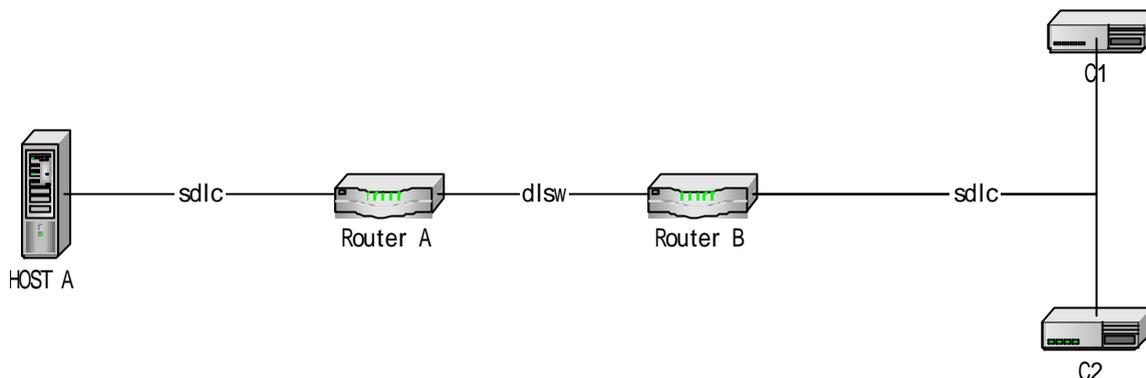
config-interface serial 0
  config-encap sdhc
  config-sdhc vmac4000.1111.0001
  config-sdhc address c1
  config-sdhc xid c1 01712345(configuringXID, as PU2.0)
  config-sdhc partner 4000.1234.00C1 c1
  
```

```

config-sdlc address c2(default configuration is PU2.1)
config-sdlc partner 4000.1234.00C2 c2
config-sdlc role primary

```

### sdlc Configuration Example 1-2



This example describes an SDLC configuration which implement the support for DLSW+.

Router A, as a local secondary station, SDLC configured as follows:

```

config-interface serial 0
  config-encap sdlc
  config-sdlc vmac4000.1234.0000
  config-sdlc address c1
  config-sdlc xid c1 01712345(configured XID as PU2.0)
  config-sdlc partner 4000.5678.00c1 c1
  config-sdlc address c2(default configuration is PU2.1)
  config-sdlc partner 4000.5678.00c2 c2
  config-sdlc role secondary

```

Router B as remote secondary station: primary station of c1 and c2, c1 and c2 reserved for DLSW+ and can not be used by any other data link user. c1 is PU2.0, c2 is PU2.1. SDLC configuration as below:

```

config-interface serial 0
  config-encap sdlc
  config-sdlc vmac4000.5678.0000
  config-sdlc address c1
  config-sdlc xid c1 01712345(configured XID as PU2.0)
  config-sdlc partner 4000.1234.00C1 c1
  config-sdlc address c2(default configuration is PU2.1)
  config-sdlc partner 4000.1234.00C2 c2
  config-sdlc role primary

```

## 11 VPDN configuration task list

In L2TP modules, VPDN sub-module contacts with VPDN group, it's mainly used for creating and managing VPDN group information, both LAC and LNS need obtain relative information from VPDN group for creating tunnel and session.

### 11.1 VPDN module encapsulation

CLIENT will not send LCP OPEN information to LAC until encapsulating VPDN module. In default setting, system VPDN function is disabled. when executing VPDN enable command, VPDN function will be enabled. command NO prohibit VPDN sub-function.

using the below command for binding VPDN module.

| Command     | Function                |
|-------------|-------------------------|
| vpdn enable | Encapsulate VPDN module |

```
[DEFAULT@Router /config/]#vpdn
```

Key Word:

U(undo) D(default) Q(quit)

(00)Enable Enable VPDN

Please Input the code of command to be excute(0-0): 0 (select Enable)

Will you excute it? (Y/N):y

### 11.2 create VPDN group

tunnel control module information can be obtained from VPDN group, it can create 300 VPDN groups at least.

Using below command for creating VPDN group:

| command                        | function          |
|--------------------------------|-------------------|
| vpdn-group <i>group number</i> | create VPDN group |

```
[DEFAULT@Router /config/]#vpdn-group
```

Key Word:

U(undo) D(default) Q(quit)

(00group\_number

Please Input the code of command to be excute(0-0): 0

Please input a string:2

Will you excute it? (Y/N):y

### 11.3 set VPDN group as LNS dial mode

VPDN group can be regarded as LAC or LNS, the following command can set VPDN group as LNS:

| command       | function                        |
|---------------|---------------------------------|
| Accept-dialin | set VPDN group as LNS dial mode |

Key Word:

Q(quit)

(00)accept\_dialin VPDN accept-dialin group configuration

(01)chinese help message in Chinese

(02)chmem Change memory of system

(03)connect Open a outgoing connection

(04)default restore default configuration

(05)disconnect Disconnect an existing outgoing network connect  
ion

(06)domain Initiate a tunnel based on domain name

(07)english help message in English

(08)exit exit / quit

(09)force-local-chap Force a CHAP challenge to be instigated locally

(10)help Description of the interactive help system

- (11)history look up history
- (12)initiate-to Initiate tunnel to remote peer
- (13)interface interface configuration
- (14)l2tp L2TP specific commands
- (15)lcp-renegotiation force LCP negotiate locally
- (16)local-name Local name used for group authentication
- (17)no negate configuration
- (18)protocol Tunneling protocol to be used
- (20)request-dialin VPDN request-dialin group configuration
- (21)resume Resume an active outgoing network connection
- (22)router routing protocol configuration
- (23)show show configuration and status
- (24)source-ip Set source IP address for this vpdn-group
- (25)telnet Open a telnet connection
- (26)terminate-from Terminate tunnel from remote peer
- (27)test
- (28)virtual-template Virtual template to clone from
- (29)where display all outgoing telnet connection

Please Input the code of command to be excute(0-29):0 ( select accept-dialin parameter )

Will you excute it? (Y/N):y

### 12.4 set VPDN group as LAC dial mode

VPDN group can be regarded as LAC or LNS, the following command can set VPDN group as LAC:

| command        | function                        |
|----------------|---------------------------------|
| Request-dialin | set VPDN group as LAC dial mode |

Key Word:

Q(quit)

.....

- (20)request-dialin VPDN request-dialin group configuration
- (21)resume Resume an active outgoing network connection
- (22)router routing protocol configuration
- (23)show show configuration and status
- (24)source-ip Set source IP address for this vpdn-group
- (25)telnet Open a telnet connection
- (26)terminate-from Terminate tunnel from remote peer
- (27)test
- (28)virtual-template Virtual template to clone from
- (29)where display all outgoing telnet connection

Please Input the code of command to be excute(0-29):20 ( select request-dialin parameter )

Will you excute it? (Y/N):y

### 12.5 protocol binding

VPDN group must bind with relative protocol, for this product, only L2TP protocol is enabled, the following command can bind VPDN group and protocol:

| command              | function                          |
|----------------------|-----------------------------------|
| Protocol <i>l2tp</i> | bind VPDN group and L2TP protocol |

Key Word:

Q(quit)

.....

- (18)protocol Tunneling protocol to be used
- (20)request-dialin VPDN request-dialin group configuration
- (21)resume Resume an active outgoing network connection
- (22)router routing protocol configuration
- (23)show show configuration and status
- (24)source-ip Set source IP address for this vpdn-group
- (25)telnet Open a telnet connection
- (26)terminate-from Terminate tunnel from remote peer
- (27)test
- (28)virtual-template Virtual template to clone from
- (29)where display all outgoing telnet connection

Please Input the code of command to be excute(0-29):18 ( select protocol parameter )

Will you excute it? (Y/N):y  
 Key Word:  
 U(undo) D(default) Q(quit)  
 (00)l2tp use L2TP protocol  
 Please Input the code of command to be excute(0-0): 0 ( select l2tp protocol )  
 Please input a string:l2tp  
 Will you excute it? (Y/N):y

#### 11.4 set LAC domain name

LAC will not response until LAC OPEN request user name in certain VPDN group domain, afterwards, sending SCCRQ information, user name should include '@' division symbol, the character after '@' is user domain name, the following command can set LAC domain name:

| command            | function            |
|--------------------|---------------------|
| Domain domain_name | set LAC domain name |

Key Word:  
 Q(quit)  
 (00)accept\_dialin VPDN accept-dialin group configuration  
 (01)chinese help message in Chinese  
 (02)chmem Change memory of system  
 (03)connect Open a outgoing connection  
 (04)default restore default configuration  
 (05)disconnect Disconnect an existing outgoing network connect ion  
 (06)domain Initiate a tunnel based on domain name  
 .....  
 Please Input the code of command to be excute(0-29):6 (select domain parameter )  
 Key Word:  
 Q(quit)  
 <00> WORD domain\_name  
 Please Input the code of command to be excute(0-1):0  
 Please input a string:bdcom (input domain name , for example bdcom )  
 Will you excute it? (Y/N):y

#### 11.5 set remote LNS connected with LAC ip address

LAC will response to the LCP OPEN request sending from CLIENT and send SCCRQ information, there must have a target LNS, so the remote LNS IP address connected with LAC should be specified. LAC can response to several LNS, the priority should arrange from low to high, if the priority is same, the IP address could be sent from low to high, if there is no response, then sending to another IP address LNS, 5 different IP address LNS can be specified totally, the priority value change from 0 to 5, the default priority is 5,the lower priority value, the higher priority. Relative command as follows:

| command                                        | function                                        |
|------------------------------------------------|-------------------------------------------------|
| Initiate-to ip ipaddr priority<br>priority_num | set remote LNS connected with LAC ip<br>address |

Key Word:  
 Q(quit)  
 .....  
 (09)force-local-chap Force a CHAP challenge to be instigated locally  
 (10)help Description of the interactive help system  
 (11)history look up history  
 (12)initiate-to Initiate tunnel to remote peer  
 .....  
 Please Input the code of command to be excute(0-29):12 (select initiate-to parameter )

```
Will you excute it? (Y/N):y
Key Word:
U(undo) D(default) Q(quit)
(00)Ip          Add IP host
Please Input the code of command to be excute(0-0): 0
Please input a ip address:192.168.18.90
Key Word:
Q(quit)
.....
(00)priority
(01)cr
Please Input the code of command to be excute(0-1):0
Key Word:
Q(quit)
<00> 5-100    priority
Please Input the code of command to be excute(0-1):0
Please input a string: 4 (input priority , for example 4)
Will you excute it? (Y/N):y
```

### 11.6 set VPDN group local tunnel name

when LAC sends SCCRQ, the local tunnel name will be sent together, thus LNS will find local VPDN group based on the remote tunnel name, the local tunnel name can include 244 bytes character string at least, relative command as follows:

| command              | function                         |
|----------------------|----------------------------------|
| Localname local name | set VPDN group local tunnel name |

```
Key Word:
U(undo) D(default) Q(quit)
.....
(13)interface interface configuration
(14)l2tp L2TP specific commands
(15)lcp-renegotiation force LCP negotiate locally
(16)local-name Local name used for group authentication
.....
Please Input the code of command to be excute(0-29): 16 (select local-name)

Please input a string: name (input local tunnel name, for example name)
Will you excute it? (Y/N):y
```

### 11.7 set remote LAC tunnel name connected with LNS

After receiving SCCRQ information, LNS will find VPDN group matching remote tunnel name with LAC tunnel name, so LNS VPDN group can configure remote tunnel name which connect with LNS for matching after receiving SCCRQ information. If a VPDN group doesn't configure remote tunnel name, this group will be regarded as default VPDN group, when there is no other matching VPDN group, this information will be adopted.

| command                        | function                                      |
|--------------------------------|-----------------------------------------------|
| Terminate-from remote_lac_name | set remote LAC tunnel name connected with LNS |

```
Key Word:
U(undo) D(default) Q(quit)
```

```

.....
(25)telnet Open a telnet connection
(26)terminate-from Terminate tunnel from remote peer
(27)test
(28)virtual-template Virtual template to clone from
(29)where display all outgoing telnet connection
Please Input the code of command to be excute(0-29): 26 (select terminate-from)
Key Word:
Q(quit)
<00> WORD      remote_lac_name
Please Input the code of command to be excute(0-1):0
Please input a string:name (input remote tunnel name, for example name)
Will you excute it? (Y/N):y

```

### 11.8 reconfirm LNS and CLIENT

after establishing session successfully and LNS authenticating instead of LAC,LNS and CLIENT can reconfirm, relative command as follows:

| command          | function                 |
|------------------|--------------------------|
| Force-local-chap | reconfirm LNS and CLIENT |

```

Key Word:
U(undo) D(default) Q(quit)
(00)accept_dialin VPDN accept-dialin group configuration
(01)chinese help message in Chinese
(02)chmem Change memory of system
(03)connect Open a outgoing connection
(04)default restore default configuration
(05)disconnect Disconnect an existing outgoing network connect ion
(06)domain Initiate a tunnel based on domain name
(07)english help message in English
(08)exit exit / quit
(09)force-local-chap Force a CHAP challenge to be instigated locally
.....
Please Input the code of command to be excute(0-29): 9 (select force-local-chap)
Will you excute it? (Y/N):y

```

### 11.9 LCP renegotiate LNS and CLIENT

After session establish successfully, LNS can renegotiate the whole PPP protocol with CLIENT. Relative command as below:

| command           | function                       |
|-------------------|--------------------------------|
| lcp-renegotiation | LCP renegotiate LNS and CLIENT |

```

Key Word:
U(undo) D(default) Q(quit)
.....
(13)interface interface configuration
(14)l2tp L2TP specific commands
(15)lcp-renegotiation force LCP negotiate locally
.....
Please Input the code of command to be excute(0-29): 15 (select lcp-renegotiation)
Will you excute it? (Y/N):y

```

### 11.10 set VPDN group source IP address

VPDN group source IP address can be specified, then source IP address at top of IP packet will send to VPDN group source IP address, however, source IP address must be the ethernet card address exists in the router, otherwise binding will fail. Relative command as below:

| command          | function                         |
|------------------|----------------------------------|
| Source-ip ipaddr | Set VPDN group source IP address |

Key Word:

U(undo) D(default) Q(quit)

.....

- (22)router routing protocol configuration
- (23)show show configuration and status
- (24)source-ip Set source IP address for this vpdn-group
- (25)telnet Open a telnet connection
- (26)terminate-from Terminate tunnel from remote peer

.....

Please Input the code of command to be excute(0-29): 24 (select source-ip)

Key Word:

Q(quit)

.....

(00)A.B.C.D IP address

Please Input the code of command to be excute(0-0): 0

Please input a ip address:192.168.18.20 (input source IP address, for example 192.168.18.20)

Will you excute it? (Y/N):y

### 11.11 clone configured source interface on LNS workgroup

After establishing session, LNS must connect with CLIENT through certain virtual interface, virtual interface number can be created virtual module interface, if this interface is not created, then creating. Relative command as below:

| command                           | function                                           |
|-----------------------------------|----------------------------------------------------|
| virtual-template virtual-temp-num | clone configured source interface on LNS workgroup |

Key Word:

U(undo) D(default) Q(quit)

.....

- (26)terminate-from Terminate tunnel from remote peer
- (27)test
- (28)virtual-template Virtual template to clone from
- (29)where display all outgoing telnet connection

Please Input the code of command to be excute(0-29): 28 (select virtual-template)

Key Word:

Q(quit)

.....

(00) virtual-temp-num

Please Input the code of command to be excute(0-0): 0

Please input a string:3 (input virtual interface number, for example 3)

Will you excute it? (Y/N):y

### 11.12 tunnel authentication

the authentication method similar to CHAP can be executed between LAC and LNS, there will not establish tunnel until passing authentication. Relative command as below:

| command | function |
|---------|----------|
|---------|----------|

|                    |                           |
|--------------------|---------------------------|
| L2tp tunnel authen | Set tunnel authentication |
|--------------------|---------------------------|

Key Word:  
 U(undo) D(default) Q(quit)  
 .....  
 (11)history look up history  
 (12)initiate-to Initiate tunnel to remote peer  
 (13)interface interface configuration  
 (14)l2tp L2TP specific commands  
 .....  
 Please Input the code of command to be excute(0-29):14 (select l2tp)  
 Key Word:  
 U(undo) D(default) Q(quit)  
 (00)tunnel L2TP tunnel commands  
 (01)hidden Allow AVPs to be hidden  
 Please Input the code of command to be excute(0-1): 0  
 Input 0 , select tunnel :  
 Key Word:  
 Q(quit)  
 (00)authentication Authenticate tunnel  
 (01)hello Hello packet interval  
 (02)password Tunnel password for authentication and/or AVP hiding  
 (03)receive-window Receive window size for control channel  
 Please Input the code of command to be excute(0-3): 0(select authentication)  
 Will you excute it? (Y/N):y

### 11.14 set tunnel password

if LNS and LAC configured tunnel authentication, the authentication will not succeed until both sides of tunnel are configured the same password, tunnel password at least includes 254 characters. The command as below:

| command                       | function            |
|-------------------------------|---------------------|
| L2tp tunnel password password | Set tunnel password |

Key Word:  
 U(undo) D(default) Q(quit)  
 .....  
 (13)interface interface configuration  
 (14)l2tp L2TP specific commands  
 .....  
 Please Input the code of command to be excute(0-29):14 (select l2tp)  
 Key Word:  
 U(undo) D(default) Q(quit)  
 (00)tunnel L2TP tunnel commands  
 (01)hidden Allow AVPs to be hidden  
 Please Input the code of command to be excute(0-1): 0  
 Input 0 , select tunnel :  
 Key Word:  
 Q(quit)  
 (00)authentication Authenticate tunnel  
 (01)hello Hello packet interval  
 (02)password Tunnel password for authentication and/or AVP hiding

(03)receive-window Receive window size for control channel  
 Please Input the code of command to be excute(0-3): 2(select password)  
 Key Word:  
 Q(quit)  
 <00> WORD password  
 Please Input the code of command to be excute(0-1):0  
 Please input a string:word (input password, for example word)  
 Will you excute it? (Y/N):y

### 11.15 set time interval of sending HELLO diagram

after session establishing successfully, LAC and LNS will send HELLO diagram to each other regularly for testing the line. The time interval of sending HELLO diagram can be assigned from 0s to 4294967294s.relative command as below:

| command                         | function                                   |
|---------------------------------|--------------------------------------------|
| L2tp tunnel hello hellointerval | set time interval of sending HELLO diagram |

[DEFAULT@Router /vpdn/]#l2tp  
 Key Word:  
 U(undo) D(default) Q(quit)  
 (00)tunnel L2TP tunnel commands  
 (01)hidden Allow AVPs to be hidden  
 Please Input the code of command to be excute(0-1): 0  
 input 0 ,select tunnel :  
 Key Word:  
 Q(quit)  
 (00)authentication Authenticate tunnel  
 (01)hello Hello packet interval  
 (02)password Tunnel password for authentication and/or AVP hiding  
 (03)receive-window Receive window size for control channel  
 Please Input the code of command to be excute(0-3): 1 (select hello)  
 Please input a string:10 (input time interval, for example 10)  
 Will you excute it? (Y/N):y

### 11.16 set tunnel accepting window size

this command is used to specify local accepting BUFFER size. At the same time, it will notify the opposite when the L2TP tunnel negotiating. the opposite station specify the sliding window size of corresponding sent diagram. The size can change from 1 to 100,

relative setting command as below :

| command                                        | function                         |
|------------------------------------------------|----------------------------------|
| L2tp tunnel receive-window receive-window-size | set tunnel accepting window size |

[DEFAULT@Router /vpdn/]#l2tp  
 Key Word:  
 U(undo) D(default) Q(quit)  
 (00)tunnel L2TP tunnel commands  
 (01)hidden Allow AVPs to be hidden  
 Please Input the code of command to be excute(0-1): 0  
 input 0 ,select tunnel :  
 Key Word:  
 Q(quit)  
 (00)authentication Authenticate tunnel

```
(01)hello          Hello packet interval
(02)password       Tunnel password for authentication and/or AVP hiding
(03)receive-window Receive window size for control channel
Please Input the code of command to be excute(0-3): 3 (select receive-window)
Will you excute it? (Y/N):y
```

### 11.17 set L2TP property hidden

if you want to change command for hidden the information, only when the tunnel password is set, this command will take effect. By default, it's not hidden, relative setting command as below:

| Command     | Function                 |
|-------------|--------------------------|
| L2tp hidden | set L2TP property hidden |

Key Word:

```
U(undo) D(default) Q(quit)
(00)accept_dialin VPDN accept-dialin group configuration
(01)chinese help message in Chinese
(02)chmem Change memory of system
(03)connect Open a outgoing connection
(04)default restore default configuration
(05)disconnect Discoonnect an existing outgoing network connection
(06)domain Initiate a tunnel based on domain name
(07)english help message in English
(08)exit exit / quit
(09)force-local-chap Force a CHAP challenge to be instigated locally
(10)help Description of the interactive help system
(11)history look up history
(12)initiate-to Initiate tunnel to remote peer
(13)interface interface configuration
(14)l2tp L2TP specific commands
```

.....

Please Input the code of command to be excute(0-29):14 (select l2tp)

Key Word:

```
U(undo) D(default) Q(quit)
(00)tunnel L2TP tunnel commands
(01)hidden Allow AVPs to be hidden
Please Input the code of command to be excute(0-1): 1 (select hidden)
Will you excute it? (Y/N):y
```

### 11.18 display VPDN group

display the created VPDN group information, relative command as follows:

| Command         | Function           |
|-----------------|--------------------|
| Show vpdn group | display VPDN group |

```
[DEFAULT@Router /config/]#show
```

Key Word:

```
U(undo) D(default) Q(quit)
.....
(45)version router version information
(46)vpdn vpdn group
(47)x25 Display X.25 state
```

.....

```

46
input 46 , select vpdn :
Key Word:
Q(quit)
(00)group      display VPDN group
Please Input the code of command to be excute(0-0): 0
Input 0 , select group
Will you excute it? (Y/N):y
The screen will display the below similar information:
!
vpdn enable
!
vpdn-group 1
accept-dialin
force-local-chap
lcp-renegotiation
terminate-from lac
l2tp hidden
l2tp tunnel authentication
local-name bdcou
protocol l2tp
    
```

### 11.19 display L2TP event information

display the control information during establishing L2TP tunnel and session. Relative command as below:

| command          | function                       |
|------------------|--------------------------------|
| Debug l2tp event | display L2TP event information |

```

[DEFAULT@Router /enable/]#debug
Key Word:
U(undo) D(default) Q(quit)
(00)aaa Debug AAA process information
.....
(12)ip IP information
(13)job Debug job information
(14)l2tp L2TP information
(15)lapb LAPB information
(16)line recv and send data on line
--More--
14
input 14 , select l2tp
Key Word:
Q(quit)
(00)error      L2TP error
(01)event      L2TP event
(02)packets    L2TP packets
Please Input the code of command to be excute(0-2): 1
Input 1 , select event :
Will you excute it? (Y/N):y
    
```

## 11.20 display L2TP packet information

display the IP packet information during establishing L2TP tunnel and session. Relative command as below:

| command           | function                        |
|-------------------|---------------------------------|
| Debug l2tp packet | Display L2TP packet information |

```
[DEFAULT@Router /enable/]#debug
```

Key Word:

U(undo) D(default) Q(quit)

(00)aaa Debug AAA process information

.....

(12)ip IP information

(13)job Debug job information

(14)l2tp L2TP information

(15)lapb LAPB information

(16)line recv and send data on line

--More--

14

input 14 , select l2tp

Key Word:

Q(quit)

(00)error L2TP error

(01)event L2TP event

(02)packets L2TP packets

Please Input the code of command to be excute(0-2): 2

Input 2 , select packets

Key Word:

Q(quit)

(00)control-packets L2TP control packets

(01)data-packets L2TP data packets

(02)detail L2TP packets detail

(03)<cr>

Please Input the code of command to be excute(0-3): 2

note: Choose as your request here, for example 2.

Will you excute it? (Y/N):y

## 11.21 display the mistake during L2TP transferring

display the mistake during establishing L2TP tunnel and session, relative command as below:

| command          | function                                     |
|------------------|----------------------------------------------|
| Debug l2tp error | display the mistake during L2TP transferring |

```
[DEFAULT@Router /enable/]#debug
```

Key Word:

U(undo) D(default) Q(quit)

(00)aaa Debug AAA process information

.....

(12)ip IP information

(13)job Debug job information

(14)l2tp L2TP information

(15)lapb LAPB information

(16)line recv and send data on line

--More--

```

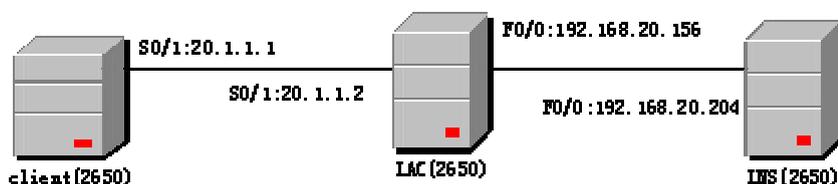
14
input 14 , select 12tp
Key Word:
Q(quit)
(00)error    L2TP error
(01)event    L2TP event
(02)packets  L2TP packets
Please Input the code of command to be excute(0-2): 0
Input 0 , select error
Will you excute it? (Y/N):y

```

## 11.22 configuration example

both the router 2650-CLIENT and serial interface 1 of 2650-LAC are encapsulated PPP protocol, LAC adopts CHAP authentication; CHAP user must input the opposite router user name in prompt; the password of two routers using CHAP must be the same, router 2650-LAC and 2650-LNS connect with each other through Ethernet interface 0.

Describe as figure 1:



configuration as below :

Client station configuration as below :

```

username ht1@bdcom.com.cn password 123
interface Serial0/0
 ip address 11.9.9.1 255.255.255.0
 ip (undo) directed-broadcast
 encapsulation ppp
 ppp chap hostname ht1@bdcom.com.cn

```

LAC configuration as below:

```

username ht1@bdcom.com.cn password 123
interface Serial0/0
 ip address 11.9.9.2 255.255.255.0
 ip (undo) directed-broadcast
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname ht1@bdcom.com.cn
 physical-layer speed 115200
 vpdn-group 1
 request-dialin
 domain bdcom.com.cn
 initiate-to ip 192.168.20.204 priority 1
 l2tp (undo) tunnel authentication
 local-name lac
 protocol l2tp
 source-ip 192.168.20.92

```

LNS configuration as below:

```
username ht1@bdcom.com.cn password 123
vpdn-group 1
  accept-dialin
  terminate-from lac
  l2tp (undo) tunnel authentication
  protocol l2tp
  virtual-template 1
```

```
interface Virtual-Template1
  ip address 11.9.9.3 255.255.255.0
  ppp authentication chap
  ppp chap hostname ht1@bdcom.com.cn
```