Network Protocol Command

Table of Content

Chapter 1 IP Address Command

1.1 IP Address Command

You can use command in this chapter to configure and check the addressing of IP network. If you want to know more information about the configuration of IP addressing, please refer to chapter “the configuration of IP addressing”.

1.1.1 arp

When configuring static ARP map, the static ARP map will be permanently saved in ARP cache. If you want to delete the configured static ARP map, use command “no arp”.

Syntas

arp ip-address hardware-address [**alias**]

no arp ip-address

Parameter

Parameter	Description
ip-address	IP address of local data link interface.
hardware-address	Physical address of local data link interface.
alias	(Optional) the router responds to the ARP request of this IP address, just like it owns this IP address.

Default

Permanent ARP map does not exist in ARP cache.

Command mode

global configuration mode

Explanation

All general hosts can support dynamic ARP analysis, so generally user does not need to specifically configure static ARP map for the host.

Example

The following command configures the MAC address of host with IP address of 1.1.1.1 as 00:12:34:56:78:90.

arp 1.1.1.1 00:12:34:56:78:90

Ralated command

clear arp-cache

1.1.2 arp timeout

Configure the duration of dynamic ARP entry in ARP cache. If you want to reset it to default value, use command no arp timeout or default arp timeout.

Syntas

arp timeout *seconds*

no arp timeout

default arp timeout

Parameter

Parameter	Description
seconds	Duration (second) of dynamic ARP entry in ARP cache. 0 means that ARP cache dynamically resoluted from this interface will not be released timeout.

Default

14400 seconds (4 hours)

Command mode

Interface configuration mode

Explanation

If you do not configure on interface without (with)ARP, then the configuration will not be effective.

Command “show interface” will display the ARP entry timeout configured on this interface, it is shown as follows:

ARP type: ARPA, ARP timeout 04:00:00

Example

The following command configures the duration of dynamic ARP map as 900 seconds on interface Ethernet 1/0, in order to more quickly refresh ARP cache.

```
interface ethernet 1/0
arp timeout 900
```

Ralated command

show interface

1.1.3 clear arp-cache

Clear all dynamic ARP cache.

Syntas

clear arp-cache

Parameter

none

Command mode

Supervisor mode

Example

The following command clears all dynamic ARP caches.

clear arp-cache

Ralated command

arp

1.1.4 ip address

Configure interface IP address, meanwhile configure network mask. Currently we do not classify A.B.C IP addresses seriously, yet do not use multicast address and broadcast address (all "1" for host part). Except Ethernet, various interfaces of other types can be on the same network. But, network configured on the Ethernet interface cannot be the same as any types of interfaces, except unnumbered interfaces . Normally you can configure one primary address and infinite secondary addresses on one interface. Secondary address can only be configured after the configuration of primary address, you can only delete primary address after delete all secondary address. IP address generated by the system itself, if the upper layer application does not designate the source address, the router will use the IP address on the same network as the gateway and configured on the outgoing interface, as the source address, if you are not sure about this IP address (such as interface router), then you can use the primary address of the outgoing interface. If one interface is not a configured IP address, and is not unnumbered interface, then this interface does not process IP packet.

If you want to delete an IP address, or stop the IP packet processing by a certain interface, you can use command "no ip address" to clear one or all IP addresses on the interface.

Syntas

ip address *ip-address mask* [**secondary**]

no ip address {*ip-address mask*}

Parameter

Parameter	Description
ip-address	IP address
mask	IP network mask
secondary	(optional) Designate that it is a configured IP secondary address, if there is no designation, it is a configured IP primary address.

Default

No configuration of any IP address on the interface

Command mode

Interface configuration mode

Explanation

If the router configures secondary IP address on certain physical segment, other systems on the same physical segment should also be configured the secondary address of the same logical network, or it will easily result in a route loop.

When using OSPFprotocol, you should guarantee that the secondary address and its primary address are in the same OSPF area.

Example

The following command configures the primary address 202.0.0.1, network mask 255.255.255.0 on Ethernet 1/0 interface, in addition, configures two IP secondary address 203.0.0.1 and 204.0.0.1.

```
interface ethernet1/0
ip address 202.0.0.1 255.255.255.0
ip address 203.0.0.1 255.255.255.0 secondary
ip address 204.0.0.1 255.255.255.0 secondary
```

1.1.5 ip directed-broadcast

Forward IP direct broadcast, and send the packet in physical broadcast form.

Syntas

ip directed-broadcast [*access-list-namer*]

no ip directed-broadcast

Parameter

Parameter	Description
access-list-name	(Optional) access list name. If the access list is defined, only the broadcast packet permits by the access list will be forwarded.

Default

It does not forward IP direct broadcast by default.

Command mode

Interface configuration mode

Example

The following example configures forwarding of IP direct broadcast on interface ethernet1/0.

interface ethernet 1/0
ip directed-broadcast

1.1.6 ip forward-protocol

When the interface is configured ip helper-address, used to designate that which UDP protocol limited broadcast packets should be forwarded.

Syntas

ip forward-protocol udp [*port*]

no ip forward-protocol udp [*port*]

default ip forward-protocol udp

Parameter

Parameter	Description
port	(Optional) the destination port which needs forwarded UDP packets.

Default

Forward the NETBIOS name service packet.

Command mode

global configuration mode

Explanation

Forward NETBIOS name service packet by default currently, if you do not want it to forward NETBIOS name service packet, you can use any of these commands:

no ip forward-protocol udp netbios-ns

no ip forward-protocol udp 137

Use the following command to stop all UDP limited broadcast packet:

no ip forward-protocol udp

Example

Router_config#ip forward-protocol udp 137

Ralated command

ip helper-address

1.1.7 ip helper-address

Forward the IP directed broadcast packets to the IP helper address designated by the command, it can be unicast or broadcast address. Each interface can be configured many helper addresses.

Syntas

ip helper-address *address*

no ip helper-address [*address*]

Parameter

Parameter	Description
address	*IP helper address*

Default

IP helper address not configured

Command mode

Interface configuration mode

Explanation

This command is not effective on X.25 interface, because the router can not discern physical broadcast.

Example

The following command configures IP helper address 1.0.0.1 on interface Ethernet 1/0.

```
interface ethernet 1/0
ip helper-address 1.0.0.1
```

Ralated command

ip forward-protocol udp

1.1.8 ip host

Define static host name-address map. If you want to delete host name-address map, use command “no ip host”.

Syntas

ip host *name address*

no ip host *name*

Parameter

Parameter	Description
name	host name
address	IP address.

Default

No maps configured

Command mode

global configuration mode

Example

The following example configures the host name as dns-server with IP address 202.96.1.3.

ip host dns-server 202.96.1.3

1.1.9 ip proxy-arp

To enable Agent ARP on the interface. If you want to close this function, use command “no ip proxy arp”.

Syntas

ip proxy-arp

no ip proxy-arp

Parameter

none

Default

Agent ARP.

Command mode

Interface configuration mode

Explanation

When the router receives ARP request, if the router has a route to the address requests IP, and the routing interface is different from the interface received request, the router will send ARP response from its own MAC address, then, when it receives actual data packets, it forwards. So, even a host does not fully realize the topological structure of the network, or it is not configured the correct(exact) route, and can communicate with the remote port. For it, remote host directly connects with it in the same physical subnetwork.

If the host requires the router to provide this service, it should be in the same IP network as the router is, or, at least its IP address should make the router consider them in the same IP subnetwork, that is to say, it can use different masks. Or, the router will not provide this service.

Example

The following example turns on the function of agent ARP on interface ethernet1/0:

interface ethernet 1/0
ip proxy-arp

1.1.10 ip unnumbered

Configure an interface as an interface with unnumbered, you can start IP process function without configuration of IP address. In order to stop IP process on this interface, use command “no ip unnumbered”.

Syntas

ip unnumbered *type number*

no ip unnumbered

Parameter

Parameter	Description
type number	The type and number of another interface configured IP address. This interface cannot be unnumbered interface using IP address of other interface.

Default

This function not started.

Command mode

Interface configuration mode

Explanation

For point-to-point link interface, you can start IP process on this interface with this command instead of configuring the exclusive IP address, and designate valid IP address on other interfaces as the source address for this interface to send packet, in order to save IP address. This kind of point-to-point interface can be called unnumbered interface. The IP packet generated on unnumbered interface, such as routing refresh packet, will use the valid IP address configured on the designated interface in the command. It also uses this address to make sure that which routing processes send update packets on this interface. But, it has the following restrictions:

- Serial interface and tunnel interface encapsulated by HDLC, PPP, LAPB, SLIP and frame relay can be configured as unnumbered interface with this command. But, X.25 and SMDS interface cannot use this command.
- No way to check whether this interface could normally operating by command “ping”. You can use “SNMP” to check the mode of this interface remotely.

This command can be realized according to the restriction that the interface cannot configure valid IP address in RFC1195.

This command can be realized according to the restriction that the interface cannot configure valid IP address in RFC1195.

Example

The following command configures interface serial1/0 as unnumbered interface, uses valid IP address 1.0.0.1 configured on interface ethernet1/1 as the source address to send packet on this interface:

interface ethernet 1/1

ip address 1.0.0.1 255.255.255.0
interface serial 1/0
ip unnumbered ethernet 1/0

1.1.11 ping

Check the availability of the host and the connectivity of the network. This is achieved by sending ICMP response request packet to the opposite port, and wait for ICMP response packet from opposite port.

Syntas

ping [**-f**] [**-i** {*source-ip-address*][**-m** {**source-interface**}] [**-j** *host1* [*host2 host3 …*]] [**–k** *host1* [*host2, host3 …*]] [**-l** *length*] [**-n** *number*] [**-r** *hops*] [**-s** *tos*] [**-t** *ttl*] [**-v**] [**-w** *waittime*] *host*

Parameter

Parameter	Description
-f	Place DF (non-fragrant packet) position. If he packet the user wants to send is greater than path MTU, the packet will be scattered by the router on the path, and send ICMP error packet to source host. If you find a network performance problem, it may be caused by smaller MTU configured on one of the nodes. You can use this option to define the minimum MTU on the path. default:Position not placed
-l	Set the source IP address default: Send main IP address of the interface.
source-ip-address	The packet uses source-ip-address as source IP address
-m	Set the IP address of certain interface adopted by the packets
source-interface	The packet uses IP address on source-interface interface as the source address.
-j host1 [**host2 host3…**]	Set loose source router. default:Not configured.
-k host1 [**host2 host3…**]	Set serious source router. default:Not configured.
-l *length*	Set the length of ICMP data in the packet. default:556 bytes.
-n *number*	Set the number of total packet sent default:5 packets.
-r *hops*	Record routes, record hops routes maximum. default:Do not record the route.
-s *tos*	Set IP TOS of packet as tos. default:0 °
-t *ttl*	Set IP TTL of the packet as ttl. default:255 °
-**v**	Detailed output. default:Brief output.
-w *waittime*	Response time to wait for each packet. default:2 seconds.
host	Destination host.

Command mode

Configure mode, global configuration mode and interface configuration mode

Explanation

Command “ping” supports destination address of broadcast address and multicast address. If it is limited broadcast (255.255.255.255) or multicast address, it will send ICMP response request packet on all available interfaces support broadcast or multicast. The router will output addresses of all response hosts. The user can directly acquire all hosts support multicast convert on directly connected session by a ping of multicast address 224.0.0.1.

IF you want to stop the ping, press “q” or “Q”.

Brief output by default:

Character	Description
!	Receive a response packet.
.	It does not receive a response in the timeout.
U	It receives ICMP destination unreachable packet
Q	It receives ICMP source refrain packet.
R	It receives ICMP redirect packet.
T	It receives ICMP timeout packet.
P	It receives ICMP parameter problem packet.

Statistical information output:

Output	Description
packets transmitted	Packets sent.
packets received	Packets received, not including other ICMP packets.
packet loss	Packet percentage not responded.
round-trip min/avg/max	Minimum/average/maximum trip time (mille-second)

Example

```
Router#ping -l 10000 -n 30 192.168.20.125
PING 192.168.20.125 (192.168.20.125): 10000 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 192.168.20.125 ping statistics ---
30 packets transmitted, 30 packets received, 0% packet loss
round-trip min/avg/max = 50/64/110 ms
```

1.1.12 show arp

Show all ARP entrys（ entries ）, including ARP map of interface IP address, static ARP map, dynamic ARP map configured by the user.

Syntas

show arp

Parameter

none

Command mode

Supervisor mode

Explanation

Displayed information includes:

potocol	Type of network address maps physical address, such as IP.
address	Address, network address maps physical address, such as IP address.
age	Survival time, the time between the generation and current of ARP entry, minute as the unit. The router use this ARP entry will not affect this value.
hardware Address	Physical address, the physical address corresponds to the network address, for irresoluted entry the value is empty.
type	Type, means the packet encapsulation type used by the interface, including ARPA, SNAP and etc…
interface	Interface, the interface related to this network address.

Example

The following command shows ARP cache

```
router#show arp
Protocol  IP Address      Age(min)  Hardware Address   Type  Interface
      IP    192.168.20.77        11   00:30:80:d5:37:e0  ARPA  Ethernet1/0
      IP    192.168.20.33         0    Incomplete
      IP    192.168.20.22         -   08:00:3e:33:33:8a  ARPA  Ethernet1/0
      IP    192.168.20.124        0   00:a0:24:9e:53:36  ARPA  Ethernet1/0
      IP    192.168.0.22          -   08:00:3e:33:33:8b  ARPA  Ethernet1/1
```

1.1.13 show hosts

Show host name—all entrys in address cache.

show hosts

Parameter

This command has no parameter or keyword.

Command mode

Configure mode

Example

The following command displays all host name/address map：

```
show hosts
```

Ralated command

clear host

1.1.14 show ip interface

Show IP configuration on the interface.

Syntas

show ip interface [*type number*]

Parameter

Parameter	Description
type	(Optional) interface type
number	(Optional) interface serial.

Command mode

Configure mode

Explanation

If the link layer of the interface can effectively send or receive data, it is a usable interface and the mode is “protocol up”. If you configure IP address on this interface, the router will add a directly connected route in the routing table. If the link layer protocol disconnects, which is “protocol down”, this directly connected route will be deleted. If you designate interface type and serial, it only displays interface information. Or, it displays IP configuration information of all interfaces.

Example

The following command shows the IP configuration on interface f0/0:

```
Router#show ip interface e0/1
  Ethernet1/0 is up, line protocol is up
    IP address : 192.168.20.167/24
    Broadcast address : 192.168.20.255
    Helper address : not set
    MTU : 1500(byte)
    Forward Directed broadcast : OFF
    Multicast reserved groups joined:
    224.0.0.9 224.0.0.6 224.0.0.5 224.0.0.2
    224.0.0.1
    Outgoing ACL : not set
    Incoming ACL : not set
    IP fast switching : ON
    IP fast switching on the same interface : OFF
    ICMP unreachables : ON
    ICMP mask replies : OFF
    ICMP redirects : ON
```

Show description:

Domain	Description
FastEthernet0/0 is up	If the interface hardware is usable, the interface is tagged “up”. If the interface is usable, its hardware and line protocol must all be “up”.
line protocol is up	If the interface can provide intercommunication, its line protocol would be tagged “up”. If the interface is usable, both the interface hardware and line protocol must be “up”.
Internet address	Interface IP address and network mask.
Broadcast address	Show broadcast address.
MTU	Show IP MTU configured on the interface.
Helper address	Show helper address/
Directed broadcast forwarding	Whether to forward directed broadcast packet.
Multicast reserved groups joined	Reserved multicast group interface joined
Outgoing access list	Outgoing access control list used by the interface.
Inbound access list	Inbound access control list used by the interface.
Proxy ARP	Whether the interface supports proxy ARP
ICMP redirects	Whether to send ICMP redirect packet on the interface
ICMP unreachables	Whether to send ICMP unreachable packets on the interface
ICMP mask replies	Whether to send ICMP mask reply packets on the interface.

1.1.15 keepalive

Check the availability of the host and the connectivity of the network. This is achieved by sending ICMP response request packet to the opposite port, but not wait for ICMP response packet from opposite port.

Syntas

keepalive [**group** group-id] [**source** source-address] [**interval** interval-time] [**number** number] **destination** destination-address

Parameter

Parameter	Description
group *group-id*	It can configure more keepalive command, and these commands are divided with group-id. Default: 0
source *source-address*	Setting the source ip address of message. Default: the host ip address of sending interface.
interval *interval-time*	The interval of sending message every time is second..缺省：1秒 Default:one second
number *number*	The number of sending message every time. Default: 5
destination *destination-address*	The objective host computer.

Command modul

Management mode and global configuration mode

Explanation

Command “keepalive” supports broadcast address and multicast address. If it is limited broadcast (255.255.255.255) or multicast address, it will send ICMP response request packet on all available interfaces support broadcast or multicast. And not wait for ICMP response packet from opposite port, it only timely send ICMP message to destination address.

Example

The following example configure two keepalive commands.

Source address 192.168.20.230 send ten ICMP request messages to destination address every ten seconds. The sending port of message is choosinged by destination address 192.168.20.1 and router protocol.

keepalive group 1 destination 192.168.20.1 source 192.168.20.230 interval 10 number 10

Source address 172.16.20.232 send five(windows default) ICMP request messages to destination address every one seconds(windows default). The sending port of message is choosinged by destination address 172.16.20.2 and router protocol.

keepalive group 2 destination 172.16.20.2 source 172.16.20.232

Chapter 2 NAT Configuration Command

2.1.1 ip nat

Use interface configuration command IP NAT to designate that the communication traffic from or to the interface obeys NAT (network address translation), if you want to prohibit the translation function of the interface, use “no” form of this command.

Note: Command “ip nat mss” only applies to ip nat outside interface, its function is to modify the MSS（Maximum Segment Size）value in TCP packet option with SYN tag from inside network. If you want to prohibit the function to modify MSS value of this interface, use “no” form of this command.

Syntas

ip nat {**inside** | **outside** | **mss** }

no ip nat {**inside** | **outside** | **mss** }

Parameter

Parameter	Description
inside	Means the interface connects to the inside network (the network obeys NAT translation).
outside	Means the interface connects to the outside network (the network obeys NAT translation).
mss	Modify MSS value (should first configure ip nat outside).

default

The communication traffic on this interface does not obey NAT.

Command mode

Interface configuration mode

Explanation

Only packets transmitted between “inside” and “outside” interfaces can be translated. You should designate at least one inside interface and one outside interface for each boundary router supposes to use NAT.

Example

The following example translated the IP address communicates between inside hosts with network address of 192.168.1.0 or 192.168.2.0 to the sole IP address in 171.69.233.208/28 network, and modifys MSS value.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
```

```
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
 ip nat mss
!
interface ethernet 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
.permit 192.168.2.0 255.255.255.0
!
```

2.1.2 ip nat enable-peek

Enable nat support for mib library. Only using the order to open support for network-manage, other clients on PC may read nat-translation statistics on Bdcom Router. At present, other clients on PC include Bdcom Net-Bar management software and Hotel management software.

Syntas

ip nat enable-peek

no ip nat enable-peek

Parameter

None

Default

Default is disable.

Command Mode

global configure state

Usage

Open support for statistics of nat-translation-information.

Example

config#ip nat enable-peek
config#no ip nat enable-peek

2.1.3 ip nat inside destination

Use global configuration command “ip nat inside destination” to start NAT of inside destination address. Use “NO” form of this command to delete the dynamic link with address pool.

Syntas

ip nat inside destination list *access-list-name* **pool** *name*

no ip nat inside destination list *access-list-name*

Parameter

Parameter	Description
list name	Name of the standard IP access list. Use global address from designated pool to translate the packet with destination address.
pool name	Name of the address pool, allocate inside local IP address from this pool during the dynamic translation.

default

Inside destination address is not translated

Command mode

global configuration mode

Explanation

This command establishes dynamic address translation in form of access list. Packets from address matched standard access list, will use the global address allocated in the designated address pool, this address pool is designated with command “ip nat pool”.

Example

In the following example, NAT use the address of net-208 pool to replace the destination address of packets matching with access list a1.

```
ip nat pool net-208 192.168.2.208 192.168.2.223 255.255.255.240
ip nat inside destination list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standar a1
 permit 171.69.233.208 255.255.255.240
!
```

2.1.4 ip nat inside source

Use global configuration command “ip nat inside source” to start NAT of inside source address. Use “no” form of this command to delete static translation or dynamic link with the pool.

Syntas

ip nat inside source {**list** *access-list-name* **pool** *name* [**overload**] | **static** *local-ip*

global-ip}

no ip nat inside source {**list** *access-list-name* **pool** *name* [**overload**] | **static** *local-ip global-ip*}

Parameter

Parameter	Description
list *access-list-name*	Name of standard IP access list. The packets whose source address corresponds with access list will be translated with global address in the address pool.
pool *name*	Name of the address pool, it dynamically allocate global IP address from this pool.
overload	(Optional) Enable the router to use one global address for many local addresses. When "overload" is set, many sessions on the same inside host will be discerned by TCP or UDP port number.
static *local-ip*	Establish an independent static address translation; this parameter establishes an allocated local address for the host on inside network. This address can be freely chosen, or allocated from RFC1918.
global-ip	Establish an independent static address translation; this parameter sets up an IP address that outside network could only access for inside host.

default

NAT of any insider source address does not exist

Command mode

global configuration mode

Explanation

This command has two forms: dynamic and static address translation. Establish dynamic translation in format of access list. Packet from address that is matching with standard access list, will use global address allocated in the designated pool to perform address translation, this pool is designated with command "ip nat pool".

As a substitution method, create an independent static address translation in grammar format with key word "STATIC".

Example

The following example translates IP address from the communication between inside hosts of 192.168.1.0 or 192.168.2.0 network to global sole IP address in 171.69.233.208/28 network.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
```

```
 ip nat outside
!
interface ethernet 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
 permit 192.168.2.0 255.255.255.0
!
```

2.1.5 ip nat local-service

The order just useful for PAT rule. On default, all packets that try to visit other network attached on other ports of the router through Nat-Outside port will be discarded. This function will prevent attack from outside network efficiently. Of course, the function will discard other normal packets, for example: remote snmp managing packet.

If packets on Nat-Outside port need be received, this order can be used to do it. The No usage can recover to default state.

Syntas

ip nat local-service {**icmp** | **udp** | **tcp** } **enable**

no ip nat local-service {**icmp** | **udp** | **tcp** } **enable**

Parameter

No parameter

Default

Default is disabled.

Command Mode

Interface configure state.

Usage

Open receiving function for ICMP/UDP/TCP.

Example

```
ip nat local-service udp enable
no ip nat local-service tcp enable
no ip nat local-service icmp enable
```

the commands will only open udp packets receiving function, and close tcp/icmp receiving function. Then, snmp packets can pass through the router to inside network.

Attention：The order just is available on NAT-Outside port. For other port, it will be no useful.

2.1.6 ip nat outside source

Use global configuration command “ip nat outside source” to start NAT of outside source address. Use “no” form of this command to delete static entry or dynamic link.

Syntas

ip nat outside source {**list** *access-list-name* **pool** *name* | **static** *global-ip local-ip*}

no ip nat outside source {**list** *access-list-name* **pool** *name* | **static** *global-ip local-ip*}

Parameter

Parameter	Description
list *access-list-name*	Name of standard IP access list. Packets with destination address matches access list will be translated with global address in the address pool.
pool *name*	Name of the pool, dynamically allocate global IP address from this list.
static *global-ip*	Establish an independent static address translation;This parameter establishes a self-owned local IP address for hosts on outside network.This address can be allocated from network address space routable globally.
local-ip	Establish an independent static address translation; This parameter establishes a local IP address of outside host accessible only by inside network for inside host. This address can be allocated from the address space routable from inside network. (mostly obeys RFC 1918) .

default

The translation from source address of outside network to inside network address does not exist

Command mode

global configuration mode

Explanation

Maybe you have used illegal and informal allocated IP address. Maybe you have chosen IP addresses that have been formally allocated to other networks. This situation where IP address is legally used (outside network) yet illegally used (inside network) is called “address overlapping”. You can use NAT to translate the inside address which overlaps with the outside address. If the IP address in your single connection network is coincidentally the same as the legal IP address allocated to other networks, and you want to communicate with these hosts or routers, you can use this function.

There are two forms of this command: dynamic and static address translation. Establish dynamic address translation in the form of access list. The packets from the address that match standard access list, will use local address allocated in the designated address pool to perform address translation, this address pool is designated with command “ip nat pool”.

As a method to replace, establish an independent static translation in grammar format with key word STATIC.

Example

The following example can translate the IP address of the communication between inside hosts from 9.114.11.0 network to global sole IP address in 171.69.233.208/28 network. Moreover, packets of outside host from network 9.114.11.0 (really existed 9.114.11.0 network) is translated in the form from network 10.0.1.0/24.

```
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 ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 9.114.11.39 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 9.114.11.0 255.255.255.0
 !
```

2.1.7 ip nat pool

Use global configuration command “ip nat pool”to define an IP address pool used for NAT. Use “no” form of this command to delete the IP address pool.

Syntas

ip nat pool name *start-ip end-ip netmask*

no ip nat pool name *start-ip end-ip netmask*

Parameter

Parameter	Description
name	Name of the pool
start-ip	Define the range of IP address pool: start address
end-ip	Define the range of IP address pool: end address
netmask	Sub-network mask. Sub-network mask tells which of the addresses belong to the network and sub-network part, yet which belong to the host part. Designate the sub-network mask of network belongs to the address in IP pool.

Default

IP pool not defined

Command mode

global configuration mode

Explanation

This command uses start address, end address and sub-network mask to define an address pool. The defined pool can be an inside global pool or an outside local address.

Example

The following example translates the IP address from the communication between inside hosts of 192.168.1.0 or 192.168.2.0 network to the global sole IP address in 171.69.233.208/28 network.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 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
 permit 192.168.2.0 255.255.255.0
```

2.1.8 ip nat translation

Use global configuration command “ip nat translation” to change the time value of NAT translation timeout. Use “no” form of this command to close the timeout.

Syntas

ip nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **max-entries** |**syn-timeout** } *seconds*

no ip nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **max-entries** |**syn-timeout** }

Parameter

Parameter	Description
timeout	Designate the timeout value of dynamic translation except overload translation. 3600 seconds by default (1hour)
udp-timeout	Designate the timeout value used on UDP interface. 300 seconds by default (5 minutes)
dns-timeout	Designate the timeout value used to connect to DNS. 60 seconds by default.
tcp-timeout	Designate the timeout value used on TCP interface. 3600 seconds by default (1 hour)
finrst-timeout	Designate the timeout value used on “finish and reset TCP” packet, this value is used to stop a connection, The default value is 60 seconds.
icmp-timeout	Set the NAT timeout value of ICMP, 60 seconds by default

max-entries	Set the maximum translation entry number of NAT, 1024 by default.
syn-timeout	Set the NAT timeout value of TCP SYN mode, 60 seconds by default.
seconds	Timeout value of translation on designated interface. The default value is the value listed in the default part.

Default

timeout is 3600 seconds (1 hours)

udp-timeout is 300 seconds (5 minutes)

dns-timeout is 60 seconds (1 minute)

tcp-timeout is 3600 seconds (1 hours)

finrst-timeout is 60 seconds (1 minute)

Command mode

global configuration mode

Explanation

After configured interface translation, because each translation entry includes more context information about using its communication traffic, you can have better control over translation entry. UDP translation of Non-domain name system (DNS) timeouts after 5 minutes, but UDP of domain name system timeouts after one minute. If there isn't RST or FIN in data stream, TCP translation timeouts after an hour; but it will timeout after one minute with RST or FIN.

Example

The following example makes UDP interface translation entry timeouts after 10 minutes.

ip nat translation udp-timeout 600

2.1.9 clear ip nat

In order to clear the statistical information of NAT, use command "clear ip nat statistics".

Syntas

clear ip nat statistics

Parameter

none

Command mode

Supervisor mode

Explanation

User this command to reset all NAT statistical information to initial mode.

Example

```
Router#show ip nat statistics
Total active translations: 1 (0 static, 0 dynamic; 1 PAT)
Outside interfaces:
 Dialer1 Virtual-access0
Inside interfaces:
 FastEthernet0/0
Dynamic mappings:
-- Inside Source
-- Outside Source
ICMP=3, UDP=29, TCP=155, FRAG_ID=5 FRAG_PTR=0 / TOTAL=192
Router#clear ip nat statistics
Router#show ip nat statistics
Total active translations: 1 (0 static, 0 dynamic; 1 PAT)
Outside interfaces:
 Dialer1 Virtual-access0
Inside interfaces:
 FastEthernet0/0
Dynamic mappings:
-- Inside Source
-- Outside Source
ICMP=0, UDP=0, TCP=0, FRAG_ID=0 FRAG_PTR=0 / TOTAL=0
```

2.1.10 clear ip nat translation

In order to clear dynamic network address translation from translation entry, use executive command “clear ip nat translation”.

Syntas

clear ip nat translation {***** | [**inside** local-ip global-ip] [**outside** local-ip global-ip]}

clear ip nat translation {**tcp|udp**} **inside** *local-ip local-port global-ip global-port* [**outside** *local-ip global-ip*]

Parameter

Parameter	Description
*	Clear all dynamic translation entrys
Inside	Clear the inside translation including designated global IP address and local IP address.
global-ip	Designate global IP address
local-ip	Designate local IP address
outside	Clear the outside translation including designated global IP address and local IP address.
tcp|udp	Protocol
global-port	Designate the global port of corresponding protocol
local-port	Designate the local port of corresponding protocol

Command mode

Supervisor mode

Explanation

Use this command can clear the dynamic translation entrys before their timeouts.

Example

The following example first shows NAT translation entry, then clears UDP translation entry:

```
Router# show ip nat translation
Pro Inside global     Inside local      Outside local     Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23  171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53
Router# show ip nat translation
Pro Inside global     Inside local      Outside local     Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23  171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

2.1.11 show ip nat statistics

Syntas

show ip nat statistics

Parameter

This command has no parameter or keyword

Command mode

Supervisor mode

Explanation

Use command “show ip nat statistics” to show NAT statistical list.

Example

The following is the output result of the example using command “show ip nat statistics” :

```
Router# show ip nat statistics
Total translations: 2 (0 static, 2 dynamic; 0 PAT)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208
 pool net-208: netmask 255.255.255.240
       start 171.69.233.208 end 171.69.233.221
       total addresses 14, allocated 2, misses 0
```

Table 9 describes the important field in output result

Figuer 2-1: Show IP NAT statistics field description

Field	Description
Total translations	The number of designated translation rule activated in the system. When an address translation rule is added, this value will be added with 1; meanwhile, when an address translation rule is cleared, this value will be deducted by 1.
Outside interfaces	Interface list of outside interfaces tagged with command “ip nat outside”.
Inside interfaces	Interface list of inside interfaces tagged with command “ip nat inside”
Expired translations	Accumulated traffic of all timeout address translations from the start of the router or last clearance of statistical inofmration.
Dynamic mappings	Information showed after it is about dynamic mappings.
Inside Source	Information about inside source address translation follows it
Access-list	Access list numbers used for address translation.
Pool	Pool name (Pool name in this example is net-208)
Netmask	IP network mask used in the pool
Start	Start IP address within address range in the pool
End	Close IP address within address range in the pool
Total addresses	Address number usable for address translation in the pool
Allocated	Address numbers allocated
Misses	address numbers not allocatable in the pool

2.1.12 show ip nat translations

Syntas

show ip nat translations [**verbose**]

Parameter

Parameter	Description
Verbose	(optional) show the extra information about each translation address list entry, include how much time it is established and how much time remained till timeout.

Command mode

Supervisor mode

Explanation

Use configure mode command “show ip nat translations” to show activated NAT address translation.

Example

The following is the output of example using command “show ip nat translation”. Several outside hosts and two inside hosts exchange packets, no overloads.

```
Router# show ip nat translations
Pro Inside local      Inside global     Outside local     Outside global
```

--- 192.168.1.95 171.69.233.209 --- ---
--- 192.168.1.89 171.69.233.210 --- --

In a situation of overloading, the address translation used for one DNS service is still activated, and the two TELNET sessions (from two different hosts) are also activated. Attention: two different inside hosts will appear in the form with same outside address.

Router# show ip nat translations
Pro Inside local Inside global Outside local Outside global
udp 192.168.1.95:1220 171.69.233.209:1220 171.69.2.132:53 171.69.2.132:53
tcp 192.168.1.89:11012 171.69.233.209:11012 171.69.1.220:23 171.69.1.220:23
tcp 192.168.1.95:1067 171.69.233.209:1067 171.69.1.161:23 171.69.1.161:23

The following is the output example with key word "verbose":

Router# show ip nat translations verbose
Pro Inside local Inside global Outside local Outside global
udp 192.168.1.95:1220 171.69.233.209:1220 171.69.2.132:53 171.69.2.132:53
create time 00:00:02, left time 00:01:10,
tcp 192.168.1.89:11012 171.69.233.209:11012 171.69.1.220:23 171.69.1.220:23
create time 00:01:13, left time 00:00:50,
tcp 192.168.1.95:1067 171.69.233.209:1067 171.69.1.161:23 171.69.1.161:23
create time 00:00:02, left time 00:53:19,

Table 10: describes the key field in output result list

Figuer 2-2 the field description of the output result of command "show IP NAT Translations"

Field	Description
Pro	Define the interface protocol of the address.
Inside global	Legal IP address(provided by NIC or ISPs), they represent one or more inside local IP address towards outside network.
Inside local	IP address allocated to the host in inside network; they may not be legal addresses provided by a NIC or ISPs.
Outside local	The IP address when an outside host looks like an inside network; they may not be the legal addresses provided by an NIC or ISPs.
Outside global	IP address of outside host allocated by its owner
Create time	The create time of address translation entry. (unit is hour: minute: second)
Left time	The timeout of address translation entry.

2.1.13 debug ip nat

Use executive command **"debug ip nat "** to debug network address translation (NAT).

Syntas

debug ip nat {detail | h323}

no debug ip nat {**detail** | **h323**}

Parameter

none

Command mode

Supervisor mode

Explanation

Using command debug ip nat detail can output the detail in output translation process, including the source, destination IP address of the packet, protocol, port number and the reason of unsuccessful translation and etc…

Example

Router# debug ip nat detail
Ethernet1/1 recv ICMP Src 194.4.4.89 Dst 10.10.10.102 no link found
Ethernet1/0 send TCP Src 194.4.4.102:2000 Dst 192.2.2.1:21 no matched rule

This table describes the domain displayed.

Domain	Description
Ethernet1/0	Type, number of the interface.
send/recv	Send/receive.
ICMP/TCP/UDP	ICMP/TCP/UDPprotocol
Src 194.4.4.102:2000	Source IP address and port number
Dst 192.2.2.1:21	Destination IP address and port number.
no link found	No link to NAT matches
no matched rule	No rule matches NAT.

First entry: ICMP packet received on Ethernet1/1 interface (the source address of it is 194.4.4.89 and the destination address is 10.10.10.102; ICMP), no corresponding NAT connection found (matching NAT rules are found)

Second entry: ICMP packet received on Ethernet1/1 interface (the source address of it is 194.4.4.102 and the destination address is 192.2.2.1; the source port of it is 2000 and the destination port is 21), no matched NAT rule found.

2.1.14 ip nat service

This command is a entrance function for the kinds of service with Nat support. It support three kinds service at present. The default service is closure.

Syntas

ip nat service { **h323** | **privateservice** | **peek** }

no ip nat service { **h323** | **privateservice** | **peek** }

Parameter

none

Default

clousure

Command mode

global configuration mode

Explanation

h323 support voip, it is used to control that Nat suppor h323.

privateservice is that Nat support net bar setting interior game server, for example: Legend and so on; it can control that Nat support private server.

peek is that Nat support net bar's interior monitor game server, it match customer software of BDCOM to scrutiny some monitor user wether leaving net.

no mode can close the relevant function.

Example

```
ip nat service privateservice
ip nat service peek
ip nat service h323
no ip nat service peek
```

2.1.15 clear ip nat statistics

This command is used to clear the statistical information of Nat.

Syntas

clear ip nat statistics

Parameter

none

Command mode

management mode

Explanation

This command can setting all statistical information of Nat to elementary state.

Note:

It only clear about the statistical parameter posterior "Packets dropped".

Example

```
Router#show ip nat statistics
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
   FastEthernet0/1
Inside interfaces:
   FastEthernet0/0
Dynamic mappings:
--Inside Source
   access-list nat
   pool natp: netmask 255.255.255.0
   start 172.16.20.125  end 172.16.20.127
```

```
   total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
   PAT(ICMP=5 UDP=39 TCP=224 MEDIA=50/ TOTAL=318), Dynamic=6
Packets dropped:
--Protocol:
   Out: tcp 123(h323 0), udp 39(h323 0), icmp 10, fragments 6
   In: tcp 46(h323 1), udp 109(h323 0), fragments 10
--Configuration:
   max entries 0, max links for all 178, max links for single 0
Router#clear ip nat statistics
Router#show ip nat statistic
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
   FastEthernet0/1
Inside interfaces:
   FastEthernet0/0
Dynamic mappings:
--Inside Source
   access-list nat
   pool natp: netmask 255.255.255.0
   start 172.16.20.125  end 172.16.20.127
   total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
   PAT(ICMP=5 UDP=39 TCP=224 MEDIA=50/ TOTAL=318), Dynamic=6
Packets dropped:
--Protocol:
   Out: tcp 0(h323 0), udp 0(h323 0), icmp 0, fragments 0
   In: tcp 0(h323 0), udp 0(h323 0), fragments 0
--Configuration:
   max entries 0, max links for all 0, max links for single 0
```

2.1.16 show ip nat users

This command is used to show how many inside-net users to pass through and their ip address.

Syntas

show ip nat users

Parameter

none

Default

none

Command mode

global configuration mode

Explanation

As this function need some operate process, if no need, please not use it.

Example

The following command performs under global mode:

show ip nat users

One possible result is:

```
                Current host count is 9, host count set is 12.
#host IP  addr  host ttl
172.16.20.67     20
172.16.20.70     55
172.16.20.81     3530
172.16.20.90     3600
```

Chapter 3 DHCP Command

3.1 DHCP Client

This chapter describes the DHCP configuration command. You can use the command introduced in this chapter to configure and monitor the operation of DHCP protocol on the router.

For information about configuration, please refer to “configure DHCP”.

3.1.1 ip address dhcp

In order to acquire an IP address for the Ethernet interface by Dynamic host configuration protocol (DHCP), you can use interface configuration command “ip address dhcp”. You can use “no” form of this command to delete the acquired IP address.

Syntas

ip address dhcp

no ip address dhcp

Parameter

none

Default

none

Command mode

Interface configuration mode

Explanation

Command “ip address dhcp” allows the interface to acquire IP address by DHCP protocol, which is extremely useful for the dynamic connection with internet service provider (ISP) by the Ethernet interface. As long as it acquires the dynamic IP address, the Ethernet can use port alteration technology (PAT) to implement network address translation (NAT).

IF the router is configured command “ip address dhcp”, the router will send “DHCP Discover” information to the DHCP server on the network.

If the router is configured command “no ip address dhcp”, the router will send “DHCP RELEASE” information.

Example

The following example enables the ethernet1/1 interface to acquire IP address of the interface by DHCPprotocol.

```
!
interface Ethernet1/1
```

ip address dhcp

Related commands

ip dhcp client

ip dhcp-server

show dhcp lease

show dhcp server

3.1.2 ip dhcp client

Configure the parameter of local router DHCP client.

Syntas

ip dhcp client { **minlease** *seconds* | **retransmit** *count* | **select** *seconds* }

no ip dhcp client { **minlease** | **retransmit** | **select** }

Parameter

Parameter	Description
minlease *seconds*	(Optional)minimum lease time acceptable, ranges from 60 seconds to 86400seconds.
ret ransmit *count*	(Optional) retransmit times of protocol packet, range from 1 to 10.
select *seconds*	(optional)time inside selected, ranges from 0 to 30.

Default

Parameter	Default value
Minlease	Default value of parameter “minlease” is 60 seconds.
Retransmit	Default value of parameter “retransmit” is 4 times.
select	Default value of parameter “select is 0 second.

Command mode

global configuration mode

Explanation

Adjust these parameters according to the requirement of the network structure and DHCPserver.

If “no” form of these commands are configured, then these parameters will be reset to the default value defined by the system.

Example

The following example configures the minimum leasing time acceptable of the DHCP client on the router to 100 seconds.

ip dhcp client minlease 100

The following example configures the retransmit times of the protocol packet of DHCP client on the router to 3 times.

ip dhcp client retransmit 3

The following example configures the interval selected of DHCP client on the router to 10 seconds.

ip dhcp client select 10

Related commands

ip address dhcp

ip dhcp-server

show dhcp lease

show dhcp server

3.1.3 ip dhcp-server

You can use command “ip dhcp-server” to designate the IP address of DHCP server which can designate the acknowledged DHCPserver.

Syntas

ip dhcp-server *ip-address*

no ip dhcp-server *ip-address*

Parameter

Parameter	Description
ip-address	IP address ofDHCPserver.

Default

Without any default IP address of DHCPserver.

Command mode

global configuration mode

Explanation

Use this command to designate an IP address of DHCPserver, the command will not replace the previously designated IP address of DHCP server.

“No” forma of this command can be used to clear the previously configured IP address of DHCPserver.

Example

The following example shows how to designate the server with IP address of 192.168.20.1 as the DHCP server on the router:

ip dhcp-server 192.168.20.1

Related commands

ip address dhcp

ip dhcp client

show dhcp lease

show dhcp server

3.1.4 show dhcp lease

You can use command “show dhcp lease” to check the allocated information of DHCP server used by the current router.

Syntas

Show dhcp lease

Parameter

none

Default

none

Command mode

Management

Explanation

Use this command to check the allocated information of DHCPserver currently used by the router.

Example

```
router#show dhcp lease
Temp IP addr: 192.168.20.3  for peer on Interface: Ethernet1/1
Temp  sub net mask: 255.255.255.0
  DHCP Lease server: 192.168.1.3, state: 4 Rebinding
  DHCP transaction id: 2049
  Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600 secs
Temp default-gateway addr: 192.168.1.2
  Next timer fires after: 02:34:26
  Retry count: 1   Client-ID: router-0030.80bb.e4c0-Et1/1
```

Related commands

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp server

debug dhcp

3.1.5 show dhcp server

You can use command “show dhcp server” to show the acknowledged information of DHCP server.

Syntas

show dhcp server

Parameter

none

Default

none

Command mode

supervisor mode

Explanation

Use this command to show the acknowledged DHCPserver information.

Example

The following example shows the acknowledged DHCPserver information.

```
router#show dhcp sever
DHCP server: 255.255.255.255
  Leases:  0
  Discovers: 62 Requests: 0     Declines: 0     Releases: 0
  Offers:    0  Acks:     0     Naks:     0     Bad:      0
  Subnet: 0.0.0.0,      Domain name:
```

Related commands

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp lease

3.1.6 debug dhcp

When dhcp is functioning on the router, you can use command “debug dhcp” to check the processing situation of dhcpprotocol.

Syntas

debug dhcp [**detail**]

no debug dhcp[**detail**]

Parameter

Parameter	Description
detail	show the packet content of DHCPprotocol.

Default

It does not show any related information by default.

Command mode

Management

Explanation

Show some important processing information about DHCP processing, example is as follows:

router#debug dhcp
router#2000-4-22 10:50:40 DHCP: Move to INIT state, xid: 0x7
2000-4-22 10:50:40 DHCP: SDISCOVER attempt # 1, sending 277 byte DHCP packet
2000-4-22 10:50:40 DHCP: B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:40 DHCP: Move to SELECTING state, xid: 0x7
2000-4-22 10:50:46 DHCP: SDISCOVER attempt # 2, sending 277 byte DHCPpacket
2000-4-22 10:50:46 DHCP: B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:54 DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket

Related commands

show dhcp lease

3.2 DHCP Sever configuration command

Configuration command for DHCPD

3.2.1 ip dhcpd ping packet

Syntas

ip dhcpd ping packet *pkgs*

Parameter

Parameter	Description
pkgs	The number of ICMP packets sent for the DHCPserver to check whether the address has been allocated.

Default

2

Command mode

global configuration mode

Explanation

The user can use the following command to configure that DHCPserver sends n ICMP packets while checking whether the address has been allocated.

ip dhcpd ping packets *n*

Example

The following command configures that DHCPserver sends 1 ICMP packet while checking whether the address has been allocated.

ip dhcpd ping packets 1

3.2.2 ip dhcpd ping timeout

Syntas

ip dhcpd ping timeout *timeout*

Parameter

Parameter	Description
timeout	Timeoutwaits for the response of ICMP packet for the DHCPserver to check whether theaddress has been allocated.

Default

5

Command mode

global configuration mode

Explanation

The user can use the following command to configure the timeout waited for the response of ICMP packet for the DHCPserver to check whether the address has been allocated as n*100ms.

ip dhcpd ping timeout *n*

Example

The user can use the following command to configure the timeout waited for the response of ICMP packet for the DHCPserver to check whether the address has been allocated as 300ms.

ip dhcpd ping timeout 3

3.2.3 ip dhcpd write-time

Syntas

ip dhcpd write-time *time*

Parameter

Parameter	Description
time	interval of DHCPserver to save the address allocation information to the database (minute as the unit)

Default

60

Command mode

global configuration mode

Explanation

The user can use the following command to configure that DHCPserver writes the address allocation information into the database every n minutes.

ip dhcpd write-time *n*

We suggest that the user do not set this value smaller than the default value.

Example

The user can use the following command to configure that DHCPserver writes the address allocation information into the database every hour.

ip dhcpd write-time 1440

3.2.4 ip dhcpd pool

Syntas

ip dhcpd pool[

Parameter

Parameter	Description
name	name of DHCP address pool

Default

none

Command mode

global configuration mode

Explanation

The user can use the following command to add a DHCP address pool named “name”, and enter into configuration mode of DHCP address pool.

ip dhcpd pool *name*

Example

The ouser can use the following command to add a DHCP address pool named “test”, meanwhile entering into configuration mode of DHCP address pool.

ip dhcpd pool test

3.2.5 ip dhcpd enable

Syntas

ip dhcpd enable

Parameter

none

Default

Close DHCP service by default

Command mode

global configuration mode

Explanation

The user can use the following command to enable DHCP service

ip dhcpd pool *name*

Example

The following command enables DHCP service.

ip dhcpd enable

3.2.6 ip dhcpd disable

Syntas

ip dhcpd disable

Parameter

none

Default

none

Command mode

global configuration mode

Explanation

The user can use the following command to disable DHCP service.

ip dhcpd disable

Example

The following command disables DHCP service.

ip dhcpd disable

3.2.7 Configuration command for DHCPD address pool

The command format for dhcpd address pool configuration is as follows:

3.2.8 network

Syntas

network *ip-addr netmask*

Parameter

Parameter	Description
ip-addr	Network address of address pool used for automatic distribution.
netmask	sub-network mask.

Default

none

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the network address of address pool used for automatic distribution. This command only applies to automatic distribution mode.

When configuring this command, insure that the network number of this “network” can be equal to that of one of IP address of the interface where the DHCP-request packet came from.

Example

The following command configures the network address of DHCP address pool as 192.168.20.0, sub-network mask as 255.255.255.0.

network 192.168.20.0 255.255.255.0

3.2.9 range

Syntas

range *low-addr high-addr*

Parameter

Parameter	Description
low-addr	The low address used to automatically allocate the address range
hogh-addr	The high address used to automatically allocate the address range

Default

none

Command mode

DHCP address pool configuration mode

Explanation

The user can use this command to configure the address range used for automatic allocation. Each address pool can be configured at most 8 ranges, and each range should be within the network. This command only applies to automatic allocation mode.

Example

The following command configures the address allocation range of DHCP address pool as 192.168.20.210－192.168.20.219.

range 192.168.20.210 192.168.20.219

3.2.10 default-router

Syntas

default-router *ip-addr*

Parameter

Parameter	Description
ip-addr	Default route allocated to the client.

Default

none

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the default route allocated to the client, the client can be configure at most 4 default routes which can be separated by spacebar.

Example

The following command configures the default route allocated to the DHCP client as 192.168.20.1

default-router 192.168.20.1

3.2.11 dns-server

Syntas

dns-server *ip-addr* …

Parameter

Parameter	Description
ip-addr	DNS serveraddress allocated to the client.

Default

none

Command mode

Configuration mode of DHCP pool address

Explanation

The user can use this command to configure the DNSserver address allocated to the client, the client can be configured 4 DNSsevers at most which can be separated by a spacebar.

Example

The following command configures the DNSsever address allocated to the client as 192.168.1.3.

dns-server 192.168.1.3

3.2.12 domain-name

Syntas

domain-name *name*

Parameter

Parameter	Description
name	Domain name allocated to theclient.

Default

none

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the domain name allocated to the client

Example

The following command configures the domain name allocated to the client as “test.bdcom”.

domain-name test.domain

3.2.13 lease

Syntas

lease {*days [hours][minutes]* | *infinite*}

Parameter

Parameter	Description
days	days allocated by the address
hours	hours allocated by the address
minutes	minutes allocated by the address
infinite	infinite allocation of the address

Default

1 day

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the time limit of the address allocated to the client.

Example

The following command configures the time limit of the address allocated to the client as 2 days and 12 hours.

Lease 2 12

3.2.14 netbios-name-server

Syntas

netbios-name-server *ip-addr*

Parameter

Parameter	Description
ip-addr	Allocate the address of netbios name server of the client.

Default

none

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the address of name server allocated to the client, the client can be configured 4 netbios name server at most which can be separated by a spacebar.

Example

The following command configures the address of netbios name server of the client as 192.168.1.10.

netbios-name-server 192.168.1.10

3.2.15 host

Syntas

host *ip-addr netmask*

Parameter

Parameter	Description
ip-addr	Host address of the address pool used for manual allocation.
netmask	Sub-network mask

Default

none

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the host address of the address pool used for manual allocation. This command only applies to the manual allocation mode and cannot configure host and range in the same address pool in the same time.

Example

The following command configures the manual allocation address of the DHCP address pool as 192.168.20.200, and the sub-network mask as 255.255.255.0.

host 192.168.20.200 255.255.255.0

3.2.16 hardware-address

Syntas

hardware-address *hardware-address*{ *type*}

Parameter

Parameter	Description
hardware-address	The hardware address used for matching the clients.
type	Hardware address type

Default

type is defaulted as 1, means Ethernet.

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the hardware address used for matching the clients, the format of the address is two hex number ab:cd:ef:gh separated by

colon. This command only applies to manual allocation mode.

Example

The following command configures the hardware address of DHCP manually allocated address pool as 10:a0:0c:13:64:7d

hardware-address 10:a0:0c:13:64:7d

3.2.17 client-identifier

Syntas

client-identifier *unique-identifier*

Parameter

Parameter	Description
unique-identifier	Client ID used for matching the clients.

Default

none

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the client ID used for matching the clients, the format of it is two hex number separated by dot: ab.cd.ef.gh. This command only applies to manual allocation mode.

Example

The following command configures the client ID of DHCP manually allocated address pool as 01:10:a0:0c:13:64:7d

client-identifier 01.10.a0.0c.13.64.7d

3.2.18 client-name

Syntas

client-name *name*

Parameter

Parameter	Description
name	the name allocated to the client

Default

none

Command mode

Configuration mode of DHCP address pool

Explanation

The user can use this command to configure the name of host used to manually allocate the clients.

Example

The following command configures the host name of the client as bdcomtect.

client-name test

3.2.19 debug ip dhcpd packet

Syntas

debug ip dhcpd packet

Parameter

none

Default

none

Command mode

Management mode

Explanation

The user can use this command to open the debug switch of data packet information of DHCPD.

Example

The following command opens the debug information output switch of DHCPD data packet.

debug ip dhcpd packet

3.2.20 debug ip dhcpd event

Syntas

debug ip dhcpd event

Parameter

none

Default

none

Command mode

Management mode

Explanation

The user can use this command to open the debug switch of DHCPD event information.

Example

The following command opens the switch of debug information output of DHCPD event.

debug ip dhcpd event

3.2.21 show ip dhcpd statistic

Syntas

show ip dhcpd statistic

Parameter

none

Default

none

Command mode

All modes except user mode

Explanation

The user can use this command to display the statistical information of DHCPD, including the amount of various packets and the addresses of automatic, manual allocation.

Example

The following command shows the statistics of DHCPD.

Show ip dhcpd statistic

3.2.22 show ip dhcpd binding

Syntas

show ip dhcpd binding {*ip-addr*}

Parameter

Parameter	Description
ip-addr	address required to show the binding information.

Default

Show all addresses of binding information

Command mode

All modes except user mode

Explanation

The user can use this command to show the address binding information of DHCPD, IP address, hardware address, binding type and timeout.

Example

The following command shows the binding information of DHCPD.

Show ip dhcpd binding

3.2.23 show ip dhcpd pool

Parameter

none

Default

none

Command mode

Other mode except user mode

Explanation

Users can use this command to show information of DHCPD address pool. It includes net number of address pool, address bound, amount of assigned address, amount of temporarily abandoned address, amount of enable assigned, handcraft assigned IP address and hardware address.

Example

The following command shows statistical information of DHCPD address pool.

show ip dhcpd pool

3.2.24 Clear ip dhcpd statistic

Syntas

Clear ip dhcpd statistic

Parameter

none

Default

none

Command mode

Management mode

Explanation

The user can use this command to delete the statistics about packet amount of DHCPD.

Example

Use the following Command to delete the statistics about packet amount of DHCPD.

Clear ip dhcpd statistic

3.2.25 Clear ip dhcpd binding

Syntas

Clear ip dhcpd binding {*ip-addr*|*}

Parameter

Parameter	Description
ip-addr	address required to delete binding information
*	delete all of the binding infomation

Default

none

Command mode

Management mode

Explanation

The user can use this command to delete the binding information of the designated

address

Example

The following command deletes the binding information of 192.168.20.210

clear ip dhcpd binding 192.168.20.210

The following command deletes the binding information of 192.168.20.210 and 192.168.20.211

clear ip dhcpd binding 192.168.20.210 192.168.20.211

The following command deletes all of the binding information

clear ip dhcpd binding *

3.2.26 clear ip dhcpd abandoned

Parameter

none

Default

None

Command mode

management mode

Explanation

This command can clear the sign of abandon.

Example

Clear ip dhcpd abandoned

Chapter 4 IP Service Command

Use the following commands to configure various IP services. For more configuration information about IP services, please refer to the chapter “configure IP services”.

4.1.1 clear tcp

Syntas

Clear a TCP connection.

clear tcp {**local** *host-name port* **remote** *host-name port* | **tcb** *address*}

Parameter

Parameter	Description
local *host-name port*	IP address of the local host and TCP port.
remote *host-name port*	IP address of the remote host and TCP port.
tcb *address*	The convert control block(TCB) of TCP connection to be deleted. TCB is the identifier of TCP connection which can be obtained by command “show tcp brief”.

Command mode

Supervisor mode

Explanation

Command “clear tcp” is mainly used to clear the closed TCP connection. In some cases, such as communication line problem, TCP connection or restart of the dealing host, TCP connection is actually stopped, but as there is no communication on TCP connection, the system cannot timely discover this situation, here you can use command “clear TCP” to close the invalid TCP connection. Among them, command clear tcp local *host-name port* remote *host-name port* is used to stop the TCP connection between designated IP address/port of local host and remote host. Command clear tcp tcb *address* is used to stop the TCP connection tagged by the designated TCB address.

Example

The following example clears the TCP connection between 192.168.20.22:23（local）&192.168.20.120:4420（remote）. Command “show tcp brief” shows the local and remote host information of current TCP connection.

```
Router#show tcp brief
TCB        Local Address        Foreign Address      State
0xE85AC8   192.168.20.22:23     192.168.20.120:4420  ESTABLISHED
0xEA38C8   192.168.20.22:23     192.168.20.125:1583  ESTABLISHED
Router#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
```

```
Router#show tcp brief
TCB        Local Address        Foreign Address      State
0xEA38C8   192.168.20.22:23      192.168.20.125:1583   ESTABLISHED
```

The following example clears the TCP connection with TCB address 0xea38c8. Command “show tcp brief” shows the TCB address of TCP connection.

```
Router#show tcp brief
TCB        Local Address        Foreign Address      State
0xEA38C8   192.168.20.22:23      192.168.20.125:1583   ESTABLISHED
Router#clear tcp tcb 0xea38c8
Router#show tcp brief
TCB        Local Address        Foreign Address      State
```

Relevant command

show tcp

show tcp brief

show tcp tcb

4.1.2 clear tcp statistics

Syntas

clear tcp statistics

Parameter

none

Command mode

Supervisor mode

Example

Use the following command to clear TCP statistics:

```
Router#clear tcp statistics
```

Relevant command

show tcp statistics

4.1.3 debug arp

Show ARP interactive information, such as sending ARP request, receiving ARP response, receiving ARP request, sending ARP response and etc… When the router cannot communicate with the host, the command can be used to analyse the ARP interactive information. Use “no debug arp” to stop showing the information.

Syntas

debug arp

no debug arp

Parameter

none

Command mode

Supervisor mode

Example

Router#debug arp

Router#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:

00:00:00:00:00, wrong cable, Ethernet1/1

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0

The first information indicates: the router receives an ARP request on interface Ethernet1/0, IP address of the host sending the request is 192.168.20.116, the MAC address is 00:90:27:a7:a9:c2, it requests the MAC address of host with IP address 192.168.20.111:

IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0

The second information means: the router receives an ARP address request from 192.168.20.139 on interface Ethernet 1/1. But, according to the interface configuration of the router, this interface is not on the network on which the host claims to be. So, there might be an error in configuration of the host. If the router sets up ARP cache according to this information, it may be unable to communication with certain host configured at the same address on the normal interface.

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:

00:00:00:00:00, wrong cable, Ethernet1/1

The third information means, the router wants to resolute the MAC address of host 192.168.20.77, so it creates an incomplete ARP entry for the host, and then fills in MAC address while receiving ARP response. According to the configuration of the router, this host connects on the interface Ethernet 1/0.

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

The fourth information means: the router sends ARP request on interface Ethernet1/0, IP address of the router is 192.168.20.22, MAC address of the interface is 08:00:3e:33:33:8a, the IP address of the requested host is 192.168.20.77. This information is related to the third information.

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0

The fifth information means, the router receives ARP response from 192.168.20.77 to router interface 192.168.20.22 on interface Ethernet1/0, which tells that its MAC address is 00:30:80:d5:37:e0. This information is related to the third and fourth information.

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0

4.1.4 debug ip icmp

Show the interactive information of Internet Control Message Protocol (ICMP). Use command “no debug ip icmp” to disable debug output.

Syntas

debug ip icmp

no debug ip icmp

Parameter

none

Command mode

Supervisor mode

Explanation

This command can show the ICMP packet the system received and sent, in order to solve the connection problem between port to port of the network. If you want to know the detailed information about command output “debug ip icmp”, please refer to RFC 792, “Internet Control Message Protocol ”.

Example

Router#debug ip icmp
Router#ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
ICMP: rcvd echo from 192.168.20.125, len 40
ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

The explanation of the first information is as follows:

ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

Domain	Description
ICMP	Shows the information of Internet Control Message Protocol (ICMP) packet.
Sent	Sending ICMP packet.

pointer indicating	ICMP packet type, this ICMP packet means that original IP packet parameter error, and also indicates the error domain. Other types of ICMP packets include: echo reply dst unreachable，include： ---net unreachable ---host unreachable ---protocol unreachable ---port unreachable ---fragmentation needed and DF set ---source route failed ---net unacknowledged ---destination host unacknowledged ---source host isolated ---net prohibited ---host prohibited ---net tos unreachable ---host tos unreachable source quench redirect,includes： ---net redirect ---host redirect ---net tos redirect ---host tos redirect echo router advertisement router solicitation time exceeded, includes: ---ttl exceeded ---reassembly timeout parameter problem，includes: ---pointer indicating ---option missed ---bad length timestamp timestamp reply information request information reply mask request mask reply If it is the ICMP type unacknowledged by the system, the system will show the ICMP type and code value.
to 192.168.20.124	The destination address of ICMP packet is 192.168.20.124, and also the source address of the original packet which initiates ICMP packet.
(dst was 192.168.20.22)	The destination address of the original packet initiates ICMP packet is 192.168.20.22.
len 48	The length of ICMP packet is 48 bytes, not including the length of IP header.

The explanation of the second information is as follows:

ICMP: rcvd echo from 192.168.20.125, len 40

Parameter	Description
rcvd	Received ICMP packet.
echo	ICMP packet type, for echo request packet.
from 192.168.20.125	The source address of ICMP packet is 192.168.20.125.

The explanation of the third information is as follows:

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

Domain	Command
src 192.168.20.22	Source address of ICMP packet is 192.168.20.22.
dst 192.168.20.125	Destination address of ICMP packet is 192.168.20.125.

According to the different types of ICMP packets, the generated ICMP packet information use different formats in the convenience of showing the packet content.

For example, for ICMP redirect packet, you can use the following format to print:

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36

ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

The first information means, it receives the redirect packet of ICMP host from host 192.168.20.77, suggests that you can use gateway 192.168.20.26 to reach the destination host 22.0.0.3, the length of ICMP packet is 36 bytes.

The second information means, it sends the redirect packet of ICMP host to 192.168.20.124, informs it to use 192.168.20.77 to reach host 22.0.0.5, the length of ICMP packet is 36 bytes.

For destination unreachable packet of ICMP, use the following formats to print:

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36

ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

The first information means, the router can not route a certain IP packet, so it sends destination host （ 202.96.209.133 ）unreachable packet of ICMP to the source host 192.168.20.124 of the packet, the length of ICMP packet is 36 bytes.

The second information means, the router receives an ICMP packet from host 192.168.20.26, informs that the destination host (2.2.2.2) is unreachable, and the length of ICMP packet is 36 bytes.

4.1.5 debug ip packet

Show the interactive information of internet protocol (IP). Use “**no debug ip packet**” to stop showing the information.

Syntas

debug ip packet [**detail**] [*ip-access-list-name*]

no debug ip packet

Parameter

Parameter	Description
detail	(Optional) output the protocol information encapsulated with IP packets, like protocol number, UDP, TCP port number, ICMP packet type and etc…
ip-access-list-name	(Optional) name of IP access list used to filter output information. Only the information meets IP packet of designated IP access list can be output.
access-group	(Optional) The name of IP access list used to filter output information. Only IP packet information meets designated IP access list will be output.
interface	(Optional) interface name used to filter output information. Only IP packets information fits with designated interface will be output.

Command mode

Supervisor mode

Explanation

This command can help to realize the final destination of every IP packets received or produced local and realize the reason of communication trouble.

Possible situations include:

Forwarded

Forwarded as broadcast packet or multicast packet

Routing failure during forwarding

Send redirect packet

Rejected as it has source routing option

Rejected as it has illegal IP options

Source route

It is required to be fragmented when sending packets from local, but DF position is reset.

Receive packet

Receive IP fragment

Send packet

Send broadcast/multicast

Routing failure for packet generated local

Packets generated local are fragmented

Received packets are filtered

Sent packets are filtered

Link layer encapsulation failure (only for Ethernet)

Unknown protocol

Using this command may result in great traffic of output information. So you'd better use it in the relatively leisure time of the router, or it will seriously affect the system

performance. What is more, you'd better use access list to filter the output, so that the system shows only the packet information that interest the user.

Example

router#debug ip packet
router#IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected
IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56, sending
IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, forward
IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

Parameter	Description
IP	Means that this information is about IP packet.
s=192.168.20.120 (Ethernet1/0)	The source address of IP packet and the interface name to receive the packet (if it is not the packet generated local)
d=19.0.0.9 (Ethernet1/0)	Destination address of IP packet and interface name of sent packet (if the routing is successful)
g=192.168.20.1	Net hop destination address of IP packet, may be gateway address, may be destination address.
len	Length of IP packet.
redirected	Means that the router will send ICMP redirect packet to the source host of this packet. Other situations include: forward---Packets are forwarded forward directed broadcast---The packets are sent as directed broadcast, packets will be transformed into physical broadcast on the sending interface. unroutable---Packet routing failure and will be discarded. source route---Source route rejected source route---System does not support source route currently, so it rejects the packet with IP source route option. bad options---IP option error and packets will be discarded. need frag but DF set---local packets need to be fragmented, but DF is reset rcvd---Packets are received local. rcvd fragment---Packet fragment received sending---sending packets generated local sending broad/multicast---sending broadcast/multicast packets generated local. Sending fragment ------Sending IP packet sent local. denied by in acl---Denied by receiving access list of the receiving interface. denied by out acl---Denied by sending access list of the sending interface. unknown protocol--- unknown protocol encapsulation failed---protocol encapsulation error, only for Ethernet. It is shown when the packets to be sent on Ethernet were discarded because of ARP resolution error.

The first information means, the router receives an IP packet, its source address is 192.168.20.120, and is from the session connected to interface Ethernet1/0, the destination address is 19.0.0.9, the sending interface defined by the routing table is Ethernet1/0, gateway address is 192.168.20.1 and the length of the packet is 60 bytes. The source hosts to discover gateway and to send IP packets are connected on the

same network, which is the network connected with interface Ethernet1/0 of the router, so the router sends out ICMP redirect packet.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected

The second information, describes the sending of ICMP redirect packet, the source address is local address 192. 168. 20.22, the destination address is the above packets' source address 192.168.20.120, sent from interface Ethernet1/0, as it is directly arriving at the destination, the gateway address is the destination address 192.168.20.120 and the length of ICMP redirect packet is 56 bytes.

IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56, sending

The third information means, the IP layer receives an IP packet and the source address of it is 192.168.20.120, the receiving interface is Ethernet1/0, the destination address of the packet is 19.0.0.9, by searching the routing table, you find out that you should forward this packet to interface Ethernet1/0, gateway is 192.168.20.77, the length packet is 60 bytes. This information shows that after the system sends ICMP redirect packet, it forwards the packet shown by the first information.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.77, len=60, forward

The fourth packet means, the IP layer receives an IP packet, whose source address is 192.168.20.81, receiving interface is Ethernet1/0, destination address is 192.168.20.22, it is an IP address configured on interface Ethernet1/0 of the router and the length of the packet is 56 bytes, received local.

IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

We are going to introduce the output of command "debug ip packet detail" in the following,

router#debug ip packet detail

router#IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67

IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89

IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0

IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

Domain	Description
UDP	Protocol name, such as UDP, ICMP, TCP and etc… Other protocols are described in protocol number.
type, code	ICMP packet type and code
src, dst	Source interface and destination interface of UDP and TCP packet.
seq	Serial of TCP packet.
ack	Acknowledgement number of TCP packet
win	Window value of TCP packet.
ACK	ACK of control bit of TCP packet is reset, means that the confirmation serial is valid. Other control bits including SYN, URG, FIN, PSH, RST.

The first information means, received UDP packet, the source port is 68, the destination port is 67.

IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67

The second information means, protocol number received the packets is 89.

IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89

The third information means, received ICMP packet, the packet type is 0, code is 0.

IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0

The fourth information means, send TCP packet, the source port is 1024, destination port is 23, serial number is 75098622, confirmation number is 161000466, size of the receiving window is 17520, the ACK tag position is reset. For information about the meaning of these domains, please refer to RFC 793— TRANSMISSION CONTROL PROTOCOL.

IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

Now we are going to introduce the usage of access control list. For example, if you want to display the packet information with source address of 192.168.20.125, first you should define standard access control list abc to only accept IP packet with source address of 192.168.20.125. Then, use this access control list in command “debug ip packet”.

Router#**config**
Router_config#ip access-list standard abc
Router_config_std_nacl#**permit 192.168.20.125**
Router_config_std_nacl#**exit**
Router_config#**exit**
Router#debug ip packet abc
Router#IP: s=192.168.20.125 (Ethernet0/1), d=192.168.20.22 (Ethernet0/1), len=48, rcvd

The above command uses the standard control access list, and it can also use extended access control list.

Relevant command

debug ip tcp packet

4.1.6 debug ip raw

Show the interactive information of internet protocol (IP). Use **“no debug ip raw”** to stop showing the information.

Syntas

debug ip raw [**detail**] [*access-list-group*] [*interface*]

no debug ip raw

Parameter

Parameter	Description
detail	(Optional) output the protocol information encapsulated by IP packet, such as protocol number, UDP, TCP port number, ICMP packet type and etc…
access-group	(Optional) the IP access list name used to filter output information. Only IP packet information meets designated IP access list will be output.
interface	(Optional) the port number used to filter output information. Only the information meets IP packet of the designated port will be output.

Command mode

Supervisor mode

Explanation

This command can help to realize the final destination of every received or local generated IP packet, and to realize the reas

Possible situations include:

Forwarded

Forwarded as broadcast packet or multicast packet

Routing failure while being forwarded

Send redirect packet

Rejected as it includes source routing option

Rejected as it includes illegal IP options

Source router

Local sent packet needs to be fragmented, but DF position is reset

Receive packet

Receive IP fragment

Send packet

Send broadcast/multicast

Routing failure of local generated packet

Local generated packets are fragmented

Received packets are filtered

Sent packets are filtered

Link layer encapsulation failure (only applies to Ethernet)

Unknown protocol

Use this command may produce great number of output information, so you'd better use it during the leisure time of the router, or it will seriously affect the system function. In addition, you should use access list to filter output if possible, and enable the system to display only the packet information that interest the user.

Example

The same as "debug ip packet"

Relevant command

debug ip tcp packet

4.1.7 debug ip rtp

Display the interactive information of header compression. Use "**no debug ip rtp**" to stop displaying the information.

Syntas

debug ip rtp {**header-compression**|**packets** |**rtcp**}

no debug ip rtp {**header-compression**|**packets** |**rtcp**}

Parameter

Parameter	Description
Header-compress	RTP/UDP/IP header compress event.
packets	RTP/UDP/IP header compress interactive data packet.
rtcp	TCP/IP header compress interactive data packet.

Command mode

Supervisor mode

Explanation

This command can help to realize the detailed process of header compress interaction.

Use this command may produce mass output information, so it is better to be used during leisure time of the router, or it will seriously affect the system performance.

Example

router # debug ip rtp header-compress
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: new connection, conn 0,
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7078, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7079, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7080, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7081, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7082, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7083, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7084, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7085, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7086, Gen = 0
2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4024, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7087, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4025, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4026, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7088, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7089, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4027, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7090, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4028, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7091, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4029, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7092, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4030, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7093, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7094, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4032, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7095, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4033, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7096, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4034, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7097, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7098, Gen

= 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4036, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7099, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4037, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7100, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4038, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7101, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: tossing error packet
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7102, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4040, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7103, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4041, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7104, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4042, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7105, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7106, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4044, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7107, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4045, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7108, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4046, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7109, Gen = 0

2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7110, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4048, Gen = 0
no deb all
1760#

4.1.8 debug ip tcp packet

Displays the received and sent information of transmit control protocol (TCP). Use “no debug ip tcp packet” to stop the display.

Syntas

debug ip tcp packet

no debug ip tcp packet

Parameter

none

Command mode

Supervisor mode

Example

Router#debug ip tcp packet
Router#tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460
DATA 1 ACK 3130379810 PSH WIN 4380
tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810
DATA 2 ACK 50659460 PSH WIN 16372
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461
DATA 50 ACK 3130379812 PSH WIN 4380
tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511
ACK 3130379812 FIN WIN 4380
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
ACK 50659511 WIN 16321
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
ACK 50659512 WIN 16321
tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
ACK 50659512 FIN WIN 16321
tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512
ACK 3130379813 WIN 4380
tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318
DATA 2 ACK 8057944 PSH WIN 17440
tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944
RST

Domain	Description
tcp:	Show the information about TCP packet.
O	Send TCP packet.

ESTABLISHED	Current mode of TCP connection. For the description of TCP connection mode, please refer to the explanation of command “debug ip tcp transactions”.
192.168.20.22:23	The source address of the packet is 192.168.20.22 and the source port is 23.
192.168.20.125:3828	The destination address of the packet is 192.168.20.125 and the destination port is 3828.
seq 50659460	Serial number of the packet is 50659460.
DATA 1	Effective data bit number included in the packet is 1.
ACK 3130379810	Acknowledgement number of the packet is 3130379810.
PSH	PSH in the control bit of the packet is reset. Other control bit including ACK, FIN, SYN, URG, and RST.
WIN 4380	The window domain of the packet is functioned to inform the size of the receiving cache of recipient’s receiving port. Currently it is 4380 bytes.
I	Receive TCP packet.

If some of above domains are not displayed, it means that this domain has no valid value in this TCP packet.

Relevant command

debug ip tcp transactions

4.1.9 debug ip tcp transactions

Display the important interactive information of convert control protocol (TCP), such as the change of TCP connection mode. Use “no debug ip tcp transactions” to stop the display.

Syntas

debug ip tcp transactions

no debug ip tcp transactions

Parameter

none

Command mode

Supervisor mode

Example

```
Router#debug ip tcp transactions
Router#TCP: rcvd connection attempt to port 23
TCP: TCB 0xE88AC8 created
TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]
TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]
TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]
TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0:0]
TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]
TCP: TCB 0xE923C8 deleted
TCP: TCB 0xE7DBC8 created
TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to
```

SYN_SENT
TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]
TCP: state was SYN_SENT -> ESTABLISHED [1022 -> 192.168.20.124:513]
TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: sending FIN [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]
TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]
TCP: TCB 0xE7DBC8 deleted

Domain	Description
TCP:	Showing the TCP interactive information.
rcvd connection attempt to port 23	Receive the connection attempt to port 23. (telnet port)
TCB 0xE88AC8 created	A new TCP connection control block, tagged “0xE88AC8”.
state was LISTEN -> SYN_RCVD	Means that the state of TCP state machine is changed from listen to LISTEN to SYN_RCVD. Possible TCP states include: LISTEN---Wait for the TCP connection attempt from any remote host. SYN_SENT--- Sending connection attempt to initiate TCP connection negotiation, and waiting for the response from recipient. SYN_RCVD---It receives the connection request and sends acknowledgement, it also sends its own connection request and waits for the recipient’s acknowledgement of connection request. ESTABLISHED---Means that the connection is set up successfully, during the data sending period, it can receive the application of upstream. FIN_WAIT_1---It has already sent the request to finish the connection, and is waiting for the acknowledgement from the recipients and the recipient’s request to finish the connection. FIN_WAIT_2--- It has already sent the request to finish the connection and received the acknowledgement from the recipients and is waiting for the recipient’s request to finish the connection. CLOSE_WAIT---It has already sent the request to finish the connection and sent the acknowledgement and is waiting for the local user to close the connection, once the user wants to close the connection, the system will send request to finish the connection. CLOSING--- It has already sent the request to finish the connection, received the request to finish the connection from the recipient and sent the acknowledgement, and is waiting for the acknowledgement of the request from the recipient to finish the connection. LAST_ACK---It has received the request from the recipient to finish the connection and acknowledged, sent the request to finish the connection is waiting for the acknowledgement. TIME_WAIT---It is waiting enough time for the confirmation that the recipient has received the acknowledgement of local request to finish connection with it, and whether the packet about this connection converted in the network has arrived at the destination or been discarded. CLOSED---Means no connection or the connection has been completely closed. For detailed information, please refer to RFC793, TRANSMISSION CONTROL PROTOCOL.

[23 -> 192.168.20.125:3828]	In the column: The first domain (23) means local TCP port The second domain（192.168.20.125）means remote IP address. The third domain (3828) means remote TCP port.
sending SYN	Send a connection attempt packet (SYN reset in TCP header control bit). Other TCP control bits include SYN, ACK, FIN, PSH, RST and URG.
seq 50658312	The serial number of sent packet is 50658312.
ack 3130379657	The acknowledge number of the sent packet is 3130379657.
rcvd FIN	Receive the request to finish the connection (FIN reset in TCP header control bit).
connection closed by user	TCP connection closed per the request of upstream application
connection timed out	Connection timed out and closed

Relevant command

debug ip tcp packet

4.1.10 debug ip udp

Show the interactive information of user data protocol (UDP). Use command “no debug ip udp” to stop.

Syntas

debug ip udp

no debug ip udp

Parameter

none

Command mode

Supervisor mode

Example

Router#debug ip udp
Router#UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32
UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008

Domain	Description
UDP:	It shows that this packet is related to UDP packet.
rcvd	Packets received
sent	Packets sent.
src	The source IP address and UDP interface of UDP packets.
dst	The target IP address and UDP interface of UDP packets.
len	The length of UDP packets.

So, the first packet means it receives a UDP packet from host 192.168.20.99, on

interface 520, the target address is 192.168.20.255, on target interface 520, and the packet length is 32 bytes.

The second packet means it sends a UDP packet, the host address is 192.168.20.22, on interface 20001, the target address is 192.168.20.43, on target interface 1001, and the packet length is 1008 bytes.

4.1.11 ip mask-reply

Demand the router to respond to IP address mask request on the designated interface. If you want to turn this function off, use command “no ip mask-reply”.

Syntas

ip mask-reply

no ip mask-reply

default ip mask-reply

Parameter

none

Default

Do not respond to the IP address mask request.

Command mode

Interface configuration mode

Example

interface ethernet 1/1
ip mask-reply

4.1.12 ip mtu

Configure the length of Maximum convert Unit of IP packets sent from the interface via command “ip mtu”. If you want to use the default value of MTU again, use command “no ip mtu”.

Syntas

ip mtu *bytes*

no ip mtu

Parameter

Parameter	Description
bytes	The maximum convert length of IP calculated by unit of byte.

Default

It is variable according to the different physical media of the interface, and is the same

as the maximum transfer unit on the interface. The minimum is 68 bytes.

Command mode

Interface configuration mode

Explanation

If the IP packet length exceeds the IP MTU set on the interface, the router would fragment the packets. For all the devices connected on the same physical media, you should configure the same protocolMTU before they can communicate. The MTU (configure by interface configuration command “mtu”) value will affect the IP MTU value. If the IP MTU value is the same as MTU value, when you change the MTU value, the IP MTU value will be automatically changed into a new MTU value. But, the change of IP MTU value will not affect the MTU value.

The minimum value of IP MTU is 68 bytes, the maximum value will not exceed the MTU configured on the interface.

Example

The following command configures the IP MTU of the interface as 200:

```
interface serial1/0
ip mtu 200
```

Relevant command

mtu

4.1.13 ip redirects

Send IP ICMP redirect packet. Use command “**no ip redirects**” to stop sending ICMP redirect packet.

Syntas

ip redirects

no ip redirects

Parameter

none

Default

Normally, IP redirect packet is sent by default. But, if the user configures hot backup routingprotocol, this function will be automatically closed. And, if the configuration of hot backup routingprotocol is canceled then, this function will not be automatically opened.

Command mode

Interface configuration mode

Explanation

When the router finds out that the forwarding interface where gateway is located is the

same as the receiving interface while forwarding packets, and the host sending packets is connected to the logical network of this interface, according to the protocol, it can send a ICMP redirect packet to inform the host to directly set the router as the gateway to the destination address of the packet without being forwarded by this router.

If the interface is configured hot backup routerprotocol, the sending of IP redirect packet may cause the loss of packets.

Example

The following command opens the function of sending ICMP redirect packet on interface Ethernet1/0:

interface ethernet 1/0
ip redirects

4.1.14 ip route-cache

Configure whether to use route cache to forward IP packet on the interface. Use command “no ip route-cache” to forbid using route cache.

Syntas

ip route-cache

no ip route-cache

ip route-cache same-interface

no ip route-cache same-interface

Parameter

Parameter	Description
same-interface	Permit IP packets to be quickly exchanged out of the receiving interface.

Default

Permit quick exchange on the interface, forbid the quick exchange on the same interface.

Command mode

Interface configuration mode

Explanation

The route cache implement load distribution on forwarded packet based on source address/destination address.

Permits route cache will enhance the packet forward performance of the router. But on low speed line (64K or lower), normally we should prohibit route cache

The user can use command “ip route-cache same-interface” to permit the IP route cache on the same interface, which means, the receiving interface is the same as the sending interface. Normally, we suggest that you do not open this function, as it is conflicted with the redirect function of the router. If the user has a not completely connected network, such as frame relay, you can enable this function on the frame relay interface. For example, routerA, B, C jointly construct a frame relay network, but

there are only links between A-B, B-C, the communication between A and C must be relayed by B: A-B-C, B receives A's packet from one DLCI of the interface, and then send it to C by another DLCI from the same interface.

Example

The following command permits the route cache on the same interface:

ip route-cache same-interface

The following command forbids route cache, including the route cache on the same interface:

no ip route-cache

The following command only forbids the route cache on the same interface:

no ip route-cache same-interface

The following command enables the system to return to the default configuration (permits route cache and forbids route cache on the same interface):

ip route-cache

Relevant command

show ip cache

4.1.15 ip source-route

Permit the router to process IP packet with IP source route option. If you require the router to discard any IP packet with IP source route option, use command "no ip source-route".

Syntas

ip source-route

no ip source-route

Parameter

none

Default

Process IP packet with IP source route option.

Command mode

global configuration mode

Example

The following command demands processing the IP packet with IP source route option.

ip source-route

Relevant command

ping

4.1.16 ip tcp synwait-time

Configure the timeout the router waits for the successful TCP connection. If you want to reset it to default time, use command "**no ip tcp synlatency time**".

Syntas

ip tcp synwait-time *seconds*

no ip tcp synwait-time

Parameter

Parameter	Description
seconds	The TCP connection waiting time counted in the unit of second. The effective value ranges from 5 to 300 seconds. 75 seconds by default.

Default

75 seconds

Command mode

global configuration mode

Explanation

When the router initiates TCP connection, if the connection is still not established successfully after latency time of TCP connection, the router considers connection failure and returns this result to the upstream application program. The user can configure the latency time for successful TCP connection, 75 seconds by default. This option has no relation with TCP connection packet forwarded by the router, but only relates to the TCP connection of the router itself.

If you want to know the current value of it, use command ip tcp synwait-time ， the value in [ ] is the current value.

Example

The following example sets the latency time for TCP connection as 30 seconds:

```
Router_config#ip tcp synwait-time 30
Router_config#ip tcp synwait-time ?
  <5-300>[30] seconds     -- wait time
```

4.1.17 ip tcp window-size

Configure the window size of TCP. If you want it to return to the default value, use command "no ip tcp window-size".

Syntas

ip tcp window-size *bytes*

no ip tcp window-size

Parameter

Parameter	Description
bytes	Window size illustrated in the unit of bit. 65535 bytes at most. 2000 bytes by default.

Default

2000 bytes

Command mode

global configuration mode

Explanation

Only if you clearly know your reason to change the default value, you'd better not change it hotheaded. If you want to know the current value, use command ip tcp window-size , the value in [] is the current value.

Example

The following example configures the TCP window size as 6000 bytes:

```
Router_config#ip tcp window-size 6000
Router_config#ip tcp window-size ?
  <1-65535>[6000] bytes     -- Window size
```

4.1.18 ip unreachables

Configure the router to send ICMP unreachable packet. If you want the router to stop sending, use command "no ip unreachables".

Syntas

ip unreachable

no ip unreachable

Parameter

none

Default

Send ICMP unreachable packet.

Command mode

Interface configuration mode

Explanation

When the router is forwarding IP packet, it may discover that there is no related routes in routing table, which results in the discard of the packet. Meanwhile, the router can

send ICMP unreachable packet to the source host, inform the source host about this situation, in order to let the source host timely discover the errors and make corrections.

Example

The following example configures to send ICMP unreachable packet on interface ethernet1/0:

```
interface ethernet 1/0
ip unreachables
```

4.1.19 show ip cache

Show route cache used for IP

Syntas

show ip cache [*prefix mask*] [*type number*]

Parameter

Parameter	Description
prefix mask	(optional) only shows the entries of which the destination address of the entry matches the designated prefix/mask the user keys in.
type number	(optional) only shows the entries of which the sending interface of the entry matches the designated interface type/number the user keys in.
rsvp	(optional) only shows the entry related to RSVP, means that, this entry, RSVP is employed.

Command mode

Supervisor mode

Example

The following example shows the route cache:

```
Router#show ip cache
Source          Destination     Interface       Next Hop
192.168.20.125  2.0.0.124       Serial1/0       2.0.0.124
192.168.20.124  192.168.30.124  Serial1/0       2.0.0.124
2.0.0.124       192.168.20.125  Ethernet1/1     192.168.20.125
```

Domain	Decription
Source	Source address.
Destination	Destination address.
Interface	Type and number of the sending interface.
Next Hop	Gateway address.

The following example shows the route cache of which the destination address matches the designated prefix/mask:

```
Router#show ip cache 192.168.20.0 255.255.255.0
Source          Destination     Interface       Next Hop
2.0.0.124       192.168.20.125  Ethernet0/1     192.168.20.125
```

The following example shows the route cache of which the sending interface matches the designated interface type/mask:

```
Router#show ip cache s1/0
Source          Destination     Interface       Next Hop
192.168.20.125  2.0.0.124       Serial1/0       2.0.0.124
192.168.20.124  192.168.30.124  Serial1/0       2.0.0.124
```

4.1.20 show ip irdp

Show socket information.

Syntas

show ip irdp

Parameter

none

Command mode

Supervisor mode

Example

```
xuhao_config_e1/0#  show ip irdp
Async0/0 ICMP router discovery protocol(IRDP) : OFF
 Ethernet1/0 ICMP router discovery protocol(IRDP) : ON
  Advertisements occur between every 450 and 600 seconds
  Advertisements are sent as broadcasts
  Advertisements valid in 1800 seconds
  Default preference : 0
Ethernet1/1 ICMP router discovery protocol(IRDP) : OFF
 Null0 ICMP router discovery protocol(IRDP) : OFF
 Loopback7 ICMP router discovery protocol(IRDP) : OFF
 Loopback10 ICMP router discovery protocol(IRDP) : OFF
```

4.1.21 show ip sockets

Show socket information.

Syntas

show ip sockets

Parameter

none

Command mode

Supervisor mode

Example

Router#show ip sockets

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590

4.1.22 show ip traffic

Show IP traffic statistics.

Syntas

show ip traffic

Parameter

none

Command mode

Supervisor mode

Example

```
Router#show ip traffic
IP statistics:
Rcvd:  0 total, 0 local destination, 0 delivered
        0 format errors, 0 checksum errors, 0 bad ttl count
        0 bad destination address, 0 unknown protocol, 0 discarded
        0 filtered , 0 bad options, 0 with options
  Opts:  0 loose source route, 0 record route, 0 strict source route
        0 timestamp, 0 router alert, 0 others
  Frags: 0 fragments, 0 reassembled, 0 dropped
        0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 0 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  230 generated, 0 forwarded
        0 filtered, 0 no route, 0 discarded
ICMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 redirect, 0 unreachable, 0 source quench
0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 parameter problem, 0 timestamps, 0 timestamp replies
0 time exceeded, 0 router solicitations, 0 router advertisements
Sent: 0 total, 0 errors
0 redirects, 0 unreachable, 0 source quench
```

0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 parameter problem, 0 timestamps, 0 timestamp replies
0 time exceeded, 0 router solicitations, 0 router advertisements

UDP statistics:
Rcvd: 28 total, 0 checksum errors, 22 no port, 0 full sock
Sent: 0 total

TCP statistics:
Rcvd: 0 total, 0 checksum errors, 0 no port
Sent: 3 total

IGMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 host queries, 0 host reports
Sent: 0 host reports

ARP statistics:
Rcvd: 8 total, 7 requests, 1 replies, 0 reverse, 0 other
Sent: 5 total, 5 requests, 0 replies (0 proxy), 0 reverse

Parameter	Description
format errors	Packet format error, such as IP header length error.
bad hop count	When the router is forwarding packets, if it finds that the TTL value is reduced to 0, the packets will be discarded.
no route	The router has no packet from corresponding route.

4.1.23 show tcp

Shows the state information of all TCP connections.

Syntas

show tcp

Parameter

none

Command mode

Supervisor mode

Example

Router#show tcp
TCB 0xE9ADC8
Connection state is ESTABLISHED, unread input bytes: 934
Local host: 192.168.20.22, Local port: 1023
Foreign host: 192.168.20.124, Foreign port: 513

Enqueued bytes for transmit: 0, input: 934 mis-ordered: 0 (0 packets)

Timer Starts Wakeup Next(ms)

Retrans 33 1 0
TimeWait 0 0 0
SendWnd 0 0 0
KeepAlive 102 0 7199500

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Domain	Description
TCB 0xE77FC8	Inside identification of TCP connection control block.
Connection state is ESTABLISHED	Current connection state. TCP connection may be in any states of the following: LISTEN---wait for the TCP connection attempt from any remote hosts. SYN_SENT---After sending connection request, waiting for the response from the recipient. SYN_RCVD---It receives the connection request and sends acknowledgement, it also sends its own connection request and waits for the recipient's acknowledgement of connection request. ESTABLISHED---Means that the connection is set up successfully, during the data sending period, it can receive the application of upstream. FIN_WAIT_1---It has already sent the request to finish the connection, and is waiting for the acknowledgement from the recipients and the recipient's request to finish the connection. FIN_WAIT_2--- It has already sent the request to finish the connection and received the acknowledgement from the recipients and is waiting for the recipient's request to finish the connection. CLOSE_WAIT---It has already sent the request to finish the connection and sent the acknowledgement and is waiting for the local user to close the connection, once the user wants to close the connection, the system will send request to finish the connection. CLOSING--- It has already sent the request to finish the connection, received the request to finish the connection from the recipient and sent the acknowledgement, and is waiting for the acknowledgement of the request from the recipient to finish the connection. LAST_ACK---It has received the request from the recipient to finish the connection and acknowledged, sent the request to finish the connection is waiting for the acknowledgement. TIME_WAIT---It waits enough time for the confirmation that the recipient has received the acknowledgement of local request to finish connection with it. CLOSED---Means no connection or the connection has been completely closed. For detailed information, please refer to RFC793, TRANSMISSION CONTROL PROTOCOL.
unread input bytes:	The data can be submitted for upstream application after the TCP procession yet has not been received by upstream application.
Local host:	Local IP address.

Local port:	Local TCP port.
Foreign host:	Remote IP address.
Foreign port:	Remote TCP port.
Enqueued bytes for transmit:	Enqueued bytes for transmission include the data sent yet not acknowledged and unsent data.
input:	Enqueued bytes for receiving: these data are waiting to be accepted for upstream application after sorting.
mis-ordered:	The bytes and packets in the mis-ordered queue, these data can only be accepted by upstream application in the receiving queue in order after other data are received. For example, if it receives packet 1,2,4,5,6, packet 1 and 2 can enter the receiving queue, but 4,5 and 6 can only enter mis-ordered queue to wait for the arrival of packet 3.

Then it shows the situation of currently connected timer, includes the start times of the timer, timeouts of the timer and the interval from the next timeout of the timer (0 means the timer is not running currently). Each connection uses independent timer. The number of timeouts of timer is normally less than the starts of the timer, because the timer may be reset during the process of running. For example, if the system receives the acknowledgement of all sent data from the recipient while the retransmit timer is running, the retransmit timer will stop running.

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

Domain	Description
Timer	Name of the timer.
Starts	Starts of the timer.
Wakeups	Timeouts of the timer.
Next(ms)	Interval from the next timeout of the timer (ms as the unit), o means the timer is not running.
Retrans	Retransmit timer, used to initiate data retransmission. The timer is started after sending the data, if the data is not acknowledged within the timeout, the timer will retransmit the data.
TimeWait	Time wait timer, used to guarantee the recipient's receiving of acknowledgement of connection stop request.
SendWnd	Send window timer, used to guarantee that the send window is reset to the normal size in the situation when TCP acknowledges loss.
KeepAlive	Keep alive timer, used to guarantee the normal operation of communication link and the recipient's still state of connection. It will ignite the sending of test packet in order to check the communication link state and the recipient's state.

Then shows the serial used by TCP connection. TCP uses serial to guarantee the reliable and ordered data convert. Local and remote hosts also perform traffic control and sending acknowledgement according to serial number.

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

Domain	Description
iss:	Initial sending serial

snduna:	Sending serial of the first bit of the data sent yet have not received the acknowledgement from the recipient.
sndnxt:	The send serial of the first bit of the data sent thereafter.
sndwnd:	TCP window size of remote host.
irs:	Initial receiving serial, which is also the initial sending serial of the remote host
rcvnxt:	Receiving serial recently acknowledged.
rcvwnd:	TCP window size of the local host.

The it shows the sending time recorded by local host, the system can adjust the system to adapt to various network according to these data.

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Domain	Description
SRTT:	Trip time after smooth treatment
RXT:	Retransmission timeout
RTV:	Variation of trip time.
MinRXT:	Minimum retransmit timeout permitted.
MaxRXT:	Maximum retransmit timeout permitted.
ACK hold:	Maximum latency of the delay of acknowledgement in order to be sent with the data.

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Domain	Description
max data segment	Maximum data segment permitted for this connection.
Rcvd	Packets received in this connection process by local host, and packets dis-ordered among them.
with data	Packets with valid data.
total data bytes	Total data bytes included in the packets.
Sent:	Total packets sent during the connection process of local host, and the packets resent.
with data	Packets include valid data.
total data bytes	Data bytes included in the packets.

Relevant command

show tcp brief

show tcp tcb

4.1.24 show tcp brief

Show brief information of TCP connection.

Syntas

show tcp brief [**all**]

Parameter

Parameter	Description
all	(optional) show all ports. If you do not input this key word, the system will not show the port in the state of “LISTEN”.

Command mode

Supervisor mode

Example

```
Router#show tcp brief
TCB        Local Address          Foreign Address        State
0xE9ADC8   192.168.20.22:1023     192.168.20.124:513     ESTABLISHED
0xEA34C8   192.168.20.22:23       192.168.20.125:1472    ESTABLISHED
```

Domain	Description
TCB	Inside tag of TCP connection.
Local Address	Local IP address and TCP port.
Foreign Address	Remote IP address and TCP port.
State	Connection mode. For detailed information please refer to command “show tcp”.

Relevant command

show tcp

show tcp tcb

4.1.25 show tcp statistics

show tcp statistics

Syntas

show tcp statistics

Parameter

none

Command mode

Supervisor mode

Example

```
Router#show tcp statistics
Rcvd: 148 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
131 packets (6974 bytes) in sequence
```

0 dup packets (0 bytes)
0 partially dup packets (0 bytes)
0 out-of-order packets (0 bytes)
0 packets (0 bytes) with data after window
0 packets after close
0 window probe packets, 0 window update packets
0 dup ack packets, 0 ack packets with unsend data
127 ack packets (247 bytes)
Sent: 239 Total, 0 urgent packets
6 control packets
123 data packets (245 bytes)
0 data packets (0 bytes) retransmitted
110 ack only packets (101 delayed)
0 window probe packets, 0 window update packets
4 Connections initiated, 0 connections accepted, 2 connections established
3 Connections closed (including 0 dropped, 1 embryonic dropped)
5 Total rxmt timeout, 0 connections dropped in rxmt timeout
1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive

Domain	Description
Rcvd:	The statistics of the packets the router received.
Total	Total packets received.
no port	The number of the received packets with non-existent ports.
checksum error	The number of the checked and wrong packets received.
bad offset	The number of the received packets with bad offset traffic.
too short	The number of the received packets with less than the minimum effective length.
packets in sequence	The number of data packets received in sequence.
dup packets	The number of duplicated packets received.
partially dup packets	The number of partly duplicated packets received.
out-of-order packets	The number of out-of-order packets received.
packets with data after window	The number of packets received with data out of the receiving window of the router.
packets after close	The number of packets received after the connection closes.
window probe packets	The number of window probe packets received.
window update packets	The number of window update packets received.
dup ack packets	The number of duplicately acknowledged packets received.
ack packets with unsent data	The number of acknowledged packets received with unsent data.
ack packets	The number of acknowledged packets received.
Sent	The statistics about the packets sent by the router.
Total	The number of total sent packets.
urgent packets	The number of urgent packets sent.
control packets	The number of control（SYN、FIN or RST） packets sent.
data packets	The number of data packets sent.
data packets retransmitted	The number of retransmitted data packets.
ack only packets	The number of acknowledged only packets sent.
window probe packets	The number of window probe packets sent.
window update packets	The number of window update packets sent.
Connections initiated	The number of connections initiated locally.

connections accepted	The number of connections accepted locally.
connections established	The number of connections established locally.
Connections closed	The number of local connections closed.
Total rxmt timeout	Total number of resent time-outs.
Connections dropped in rxmit timeout	Total number of connections dropped resulted from resent time-outs
Keepalive timeout	The number of keepalive time-outs.
keepalive probe	The number of Keepalive probe packets sent.
Connections dropped in keepalive	The number of connections dropped because of keepalive.

Relevant command

clear tcp statistics

4.1.26 show tcp tcb

Display the mode information of certain TCP connection.

Syntas

show tcp tcb *address*

Parameter

Parameter	Description
address	The convert control block (TCB) address connected with TCP to be shown. TCB is the inside TCP connection tag of the system, which can be obtained via command “show tcp brief”.

Command mode

Supervisor mode

Example

For detailed explanation of the following displayed, please refer to command “show tcp”

```
Router_config#show tcp tcb 0xea38c8

TCB 0xEA38C8
Connection state is ESTABLISHED, unread input bytes: 0
Local host: 192.168.20.22, Local port: 23
Foreign host: 192.168.20.125, Foreign port: 1583

Enqueued bytes for transmit: 0, input: 0  mis-ordered: 0 (0 packets)

Timer        Starts    Wakeups          Next(ms)
Retrans         4         0               0
TimeWait        0         0               0
SendWnd         0         0               0
KeepAlive       +5        0           6633000
```

iss: 10431492 snduna: 10431573 sndnxt: 10431573 sndwnd: 17440
irs: 915717885 rcvnxt: 915717889 rcvwnd: 4380

SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3
Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80

Relevant command

show tcp

show tcp brief

Chapter 5 Access-list Command

5.1.1 deny

This command can be used in IP access list configuration mode to configure prohibit regulations. Add a prefix “no” in front of the command to delete “deny” regulation from the ip access-list.

Syntas

deny *source* [*source-mask*] [**log**]

no deny *source* [*source-mask*] [**log**]

deny *protocol* **source** *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

no deny *protocol* **source** *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

The following syntax can also be used for internet control massage protocol(ICMP):

deny icmp source *source-mask* **destination** *destination-mask* [*icmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

The following syntax can be used for internet group management protocol (ICMP):

deny igmp source *source-mask* **destination** *destination-mask* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

The following syntax can be used for TCP:

deny tcp source *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

The following syntax can be used for data gram protocol(UDP):

deny udp source *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**precedence** *precedence*] [**tos** *tos]* [**log**]

Parameter

Parameter	Description
protocol	Protocol name or protocol number. It can be a key word like icmp, igmp, igrp, ip, ospf, tcp or udp. It can also be a whole number among 0-255 that refers to the IP protocol number. Use key word “ip” to match any Internet protocol (including ICMP, TCP and UDP). Some protocols are allowed to be restricted further as the following.
source	Source network or host number. There are 2 ways to designate the source: 32-digit binary number, decimal number separated with 4 dots. Use key word “any” to be the abbreviation of source and source Mask of 0.0.0.0 0.0.0.0
source-mask	Source address network mask. Use key word “any” to be the abbreviation of source and source Mask of 0.0.0.0 0.0.0.0 .

destination	Destination or host number. There are 2 ways to designate: Decimal number separated with 4 dots and 32-digit binary number. Use key word “any” to be the abbreviation of destination and destination Mask of 0.0.0.0 0.0.0.0 .
destination-mask	Destination address network mask. Use key word “any” to be the abbreviation of destination address and destination address Mask of 0.0.0.0 0.0.0.0 .
precedence *precedence*	(Optional) Package can be filtered by priority and designated by a number among 0-7.
tos *tos*	(Optional) Data package can use service level filter. Use a number among 0-15 to designate.
icmp-type	(Optional) ICMP package can be filtered by ICMP packet type. The type is a number among 0-255.
igmp-type	(Optional) ICMP package can be filtered by ICMP packet type or name. The type is a number among 0-15.
operator	(Optional) Compare source or destination interface. Operations include lt (smaller than), gt (bigger than), eq (equals to), neq (doesn’t equal to). If operating symbol is placed after source and source-mask, it should match the source interface. If operating symbol is placed after destination and destination-mask, it should match the destination interface.
port	(Optional) Decimal number or name of TCP or UDP interface. Interface number is a number among 0-65535. TCP interface name is listed in the part “Using Guideline”. TCP interface name can be used only to filter TCP. UDP interface name is also listed in the part “Using Instruction”. Only TCP interface name can be used to filter UDP.
established	(Optional) Indicates an established connection for TCP protocol only. Matching will occur where ACK or RST location of TCP data gram is set. Initiate TCP data gram in non-match situation to form a connection.
log	(Optional) Log can be recorded.

Command mode

IP access-list configuration state

Explanation

Access-list can be used to control the transmission of data package on the interface, control line access to virtual terminals. Stop checking extended access-list after the matching occurs. It is IP packages divided by sections but not initial sections that will be received by any extended IP access-list at once. Extended access-list is used to control accessing virtual terminal line or restricting routes from choosing update content. It is not necessary to match TCP source interface, type of service value and priority of package.

Notes:

After the initial establishment of an access-list, any follow-up addition (can be keyed in at a terminal) should be placed at the end of the list.

TCP interface name used to replace interface number is shown as below. Find out reference related to these protocols regarding current allocation number RFC. Interface number relevant to these protocols can also be found out by keying in a “?” to replace interface number.

- bgp
- ftp
- ftp-data

- login
- pop2
- pop3
- smtp
- telnet
- www

UDP interface name used to replace interface number is shown as below. Find out reference related to these protocols regarding current allocation number RFC. Interface number relevant to these protocols can also be found out by keying in a “?” to replace interface number.

- domain
- snmp
- syslog
- tftp

Example

The following example prohibits the network 192.168.5.0:

ip access-list standard filter
deny 192.168.5.0 255.255.255.0

Notes:

IP access-list ends with connotative “deny” regulation.

Ralated command

ip access-group

ip access-list

permit

show ip access-list

5.1.2 ip access-group

Use interface configuration command “ip access-group” to control accessing an interface. Use “no” format command to delete this designated access group.

Syntas

ip access-group {*access-list-name*}{**in** | **out**}

no ip access-group {*access-list-name*}{**in** | **out**}

Parameter

Parameter	Description
Access-list-name	Name of access-list. This is a character string with 20 characters at most.
in	Use access-list when entering in the interface.

out	Use access-list when going out of the interface.

Command mode

interface configuration state

Explanation

Access-list can be used either in the out-interface or in the in-interface. For standard entrance access-list, source address of the package will be checked regarding to access-list after the package is received. For extended access-list, this router also checks destination address. If the address is permitted by access-list, the software will continue to work on the package. If the address is not permitted by the access-list, this software will give up the package and return a packet showing ICMP host is not reachable.

For standard exit access-list, source address of the package will be checked by software regarding to access-list after receiving and routing a package to the control interface. For extended access-list, this router also checks access-list at the receiving end. If the address is permitted by access-list, it will transmit the package. If the address is not permitted by the access-list, this software will give up the package and return a packet showing ICMP host is not reachable.

If the designated access-list doesn't exist, all packages are permitted to pass.

Example

In the below example, list filter is applied on the package exist of Ethernet interface 1/0:

```
interface ethernet 1/0
ip access-group filter out
```

Ralated command

ip access-list

show ip access-list

5.1.3 ip access-list

Entering the IP access-list configuration mode after using this command. Access regulations can be added or deleted. Command "exit" is used to return to configuration state.

Use prefix "no" to delete IP access-list.

Syntas

ip access-list {**standard** | **extended**} *name*

no ip access-list {**standard** | **extended**} *name*

Parameter

Parameter	Description
standard	Designated as standard access-list.
extended	Designated as extended access-list.

name	Name of access-list. It is a character string of 20 characters at most.

Default

No IP access-list is defined.

Command mode

global configuration mode

Explanation

Use this command to enter IP access-list configuration mode. Command "**deny**" or "permit" can be used to configure access regulation.

Example

The following example is the configuration of a standard access-list.

ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any

Ralated command

deny

ip access-group

permit

show ip access-list

5.1.4 permit

This command can be used to configure permit regulation in IP access-list configuration mode. Add a prefix "no" in the front of the command to delete permit regulation from IP access-list.

Syntas

permit source *source-mask* **log**

no permit source *source-mask* **log**

permit protocol source *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

no permit protocol source *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

For internet control massage protocol (ICMP), the following syntax can also be used:

permit icmp source *source-mask* **destination** *destination-mask* [*icmp-type*] [**precedence** *precedence*] [**tos** *tos*] [*log*]

For internet group management protocol (IGMP), the following syntax can also be used:

permit igmp source *source-mask* **destination** *destination-mask* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For TGP, the following syntax can also be used:

permit tcp source *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [*log*]

For data gram protocol (UDP), the following syntax can also be used:

permit udp source *source-mask* [**operator port** [*port*]] **destination** *destination-mask* [**operator** *port]* [**precedence** *precedence*] [**tos** *tos*] [**log**]

Parameter

Parameter	Description
protocol	Protocol name or protocol number. It can be key word like icmp, igmp, igrp, ip, ospf, tcp or udp. It can also be a whole number among 0-255 that refers to the IP protocol number. Use key word "ip" to match any Internet protocol (including ICMP, TCP and UDP). Some protocols are allowed to be restricted further as the following.
source	Source network or host number. There are 2 ways to designate the source: 32-digit binary number, decimal number separated with 4 dots. Use key word "any" to be the abbreviation of source and source Mask of 0.0.0.0 0.0.0.0
source-mask	Source address network mask. Use key word "any" to be the abbreviation of source and source Mask of 0.0.0.0 0.0.0.0 .
destination	Destination or host number. There are 2 ways to designate: Decimal number separated with 4 dots and 32-digit binary number. Use key word "any" to be the abbreviation of source and source Mask of 0.0.0.0 0.0.0.0 .
destination-mask	Destination address network mask. Use key word "any" to be the abbreviation of destination address and destination address Mask of 0.0.0.0 0.0.0.0 .
precedence *precedence*	(Optional) Package can be filtered by priority and designated by a number among 0-7.
tos *tos*	(Optional) Data package can use service level filter. Use a number among 0-15 to designate.
icmp-type	(Optional) ICMP package can be filtered by ICMP packet type. The type is a number among 0-255.
igmp-type	(Optional) ICMP package can be filtered by ICMP packet type or name. The type is a number among 0-15.
operator	(Optional) Compare source or destination interface. Operations include lt (smaller than), gt(bigger than), eq(equals to), neq(doesn't equal to). If operating symbol is placed after source and source-mask, it should match the source interface. If operating symbol is placed after destination and destination-mask, it should match the destination interface.
port	(Optional) Decimal number or name of TCP or UDP interface. Interface number is a number among 0-65535. TCP interface name is listed in the part "Using the Guideline". TCP interface name can be used only to filter TCP. UDP interface name is also listed in the part "Using Instruction". Only TCP interface name can be used to filter UDP.
established	(Optional) Indicates an established connection for TCP protocol only. Matching will occur where ACK or RST location of TCP data gram is set. Initiate TCP data gram in non-match situation to form a connection.
log	(Optional) Log can be recorded.

Command mode

IP access-list configuration mode

Explanation

Access-list can be used to control the transmission of data package on the interface, control line access to virtual terminals. Stop checking extended access-list after the matching occurs.

It is IP packages divided by sections but not initial sections that will be received by any extended IP access-list at once. Extended access-list is used to control accessing virtual terminal line or restrict routes from choosing update content. It is not necessary to match TCP source interface, type of service value and priority of package.

Notes:

After the initial establishment of an access-list, any follow-up addition (can be keyed in at a terminal) should be placed at the end of the list.

TCP interface name used to replace interface number is shown as below. Find out reference related to these protocols regarding current allocation number RFC. Interface number relevant to these protocols can also be found out by keying in a “?” to replace interface number.

- bgp
- ftp
- ftp-data
- login
- pop2
- pop3
- smtp
- telnet
- www

UDP interface name used to replace interface number is shown as below. Find out reference related to these protocols regarding the current allocation number RFC. Interface number relevant to these protocols can also be found out by keying in a “?” to replace interface number.

- domain
- snmp
- syslog
- tftp

Example

The following example permits the network 192.168.5.0:

ip access-list standard filter
permit 192.168.5.0 255.255.255.0

Notes:

IP access-list is ended with connotative “deny” regulation.

Ralated command

- deny
- ip access-group

- ip access-list
- show ip access-list

5.1.5 show ip access-list

Use command “show ip access-list” to show current IP access-list content.

Syntas

show ip access-list[*access-list-name*]

Parameter

Parameter	Description
access-list-name	Name of access-list. This is a character string of 20 characters at most.

Default

Show all standards and extended IP access-lists.

Command mode

Supervisor mode

Explanation

Command “show ip access-list” allows you to designate a specific access-list.

Example

The following is an example output of command “show ip access-list” when the name is not designated.

```
Router# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

The following is an example output of command “show ip access-list” when the name is designated.

```
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```