**D-Link Router Family Frequently Asked Questions (FAQ)**

**Part I: General Product Overview Questions**

1. What is the Router product family?

   The Router family of products are a set of multiprotocol remote access routers that deliver a feature-rich, reliable, and secure interconnection between your LAN and the remote network such as Internet or Corporate network via ISDN. The Router product's unique features make the interconnection flexible and easy to upgrade. Router supports IP routing, IPX routing, and Transparent Bridging. It supports Ethernet, ISDN, and POTS port. Router can be managed via either RS-232 or Telnet. Its menu-driven System Management Terminal provides an easy-to-use interface.

2. What ISDN switches and B Channel protocols are supported by the Router?

   The Router supports the following ISDN switches:

   European switches:
   - DSS1 (also used in other countries)
   - 1TR6

   North American switches:
   - AT&T: NI1, Point-to-Point, Point to Multipoint
   - Northern Telecom DMS100: NI1, Custom

   The Router supports the PPP protocol in the B channels.

3. What are some of the major applications for the Router?

   Some of the major applications of the Router include:

   Internet Access
   The Router can be set up to access the Internet in 15 minutes. In addition, the Router provides an economic way for small office to connect to Internet (see Subject 8 for Internet Single User Account).

   LAN-to-LAN Connection
   The Router can dial to or answer calls from another remote access router connected to a different network. The Router supports TCP/IP, Novell IPX routing and has the capability to bridge any Ethernet protocol.

   Telecommuting Server
   The Router allows remote users to dial-in and gain access to your LAN. This feature enables users that have workstations with remote access capabilities, e.g., Windows 95, to access the network resources without physically being in the office.

4. What are the benefits of the Router over other vendors' products?

The Router incorporates features not present on most of their competitors' products.

Internet Single User Account (SUA) Support
Please see Subject 9 for details.

Multiprotocol Router
The Router is the only remote access router supporting IP Routing, IPX routing, and Transparent Bridge.

Telecommuting Server
In addition to providing both ISDN and modem access for remote users, the Router also support dynamic IP address assignment and Windows 95 compatibility. This makes the Router an ideal product for serving Windows 95 telecommuter and mobile users. The Router offers support for these accounts that will allow multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single user.

5. What other Remote Access Servers are compatible with the Router?

The Router has successfully gone through PPP MP compatibility tests with 30+ vendors in October, 1996 at Pacific Bell. Furthermore, the Router has been tested extensively with Cisco routers and Ascend routers (both Max and Pipeline).

6. How to do factory reset for the router?

There is a file called “default.cfg” which be included with shipping diskette. Use this file to restore to the factory setting. Select SMT Menu 24.6 'Restore Configuration' and transfer this file by X-modem file transfer. After file download complete, the router is in factory setting.

**Part II: Application Setup Questions**

1. What does my computer need to connect to the Router?

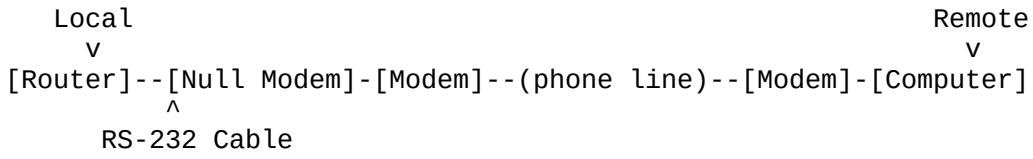
You will need an ethernet card that supports a 10baseT (RJ-45 jack) ethernet interface.
If you intend to connect your computer directly to the Router without a hub in between, you will need to use a ‘crossover’ cable and a 10baseT ethernet card. The ‘crossover’ cable is a 4-pair RJ-45 cable with pins #1 and #3 swapped, and pins #2 and #6 swapped.

To initially configure your Router, you need to have an RS-232 cable and a communications program on your computer.

In order to access the WAN (Wide Area Network) on the Router's ISDN connection, you need to have a Ethernet connection in your computer.

2. How can I remotely configure my Router using a modem?

You can configure your Router remotely through a modem call.
This setup requires an external 'local' modem.




The procedure for this setting up this application is as follows:

- Set the modem on the 'local' end to IGNORE DTR
- Set the modem on the 'local' end to Auto Answer (ATS0=1)
- Set the Router Port Speed (menu 24.2) to be 19200 if the 'local' modem is a 14.4K, and 38400 if it is faster ( 28.8K+)
- Dial the 'local' modem with the 'remote' modem.

3. How can I set up my Router as an Internet Firewall?

The Router has easily customizable filter sets that you can use to set it up as an Internet Firewall. To do this, set the filters to do the following:

Allow ARP/ICMP/PING packets
Allow TCP/UDP traffic to ports > 1023
Allow HTTP, SMTP, NNTP, DNS
Block everything else inbound from the Internet

Here's an example in Router:
A branch office wants to allow all Packet from headquarter through Internet, but would like to setup a Internet firewall to block other intrusion:

a. Allow all packets from headquarter 192.168.1.0/24 network

Menu 21.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes

IP Protocol= 0 IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 0
Port # Comp= None
Source: IP Addr= 192.168.1.0
IP Mask= 255.255.255.0
Port #= 0
Port # Comp= None
TCP Estab= N/A
More= No Log= None
Action Matched= Forward
^^^^^^^^
Action Not Matched= Check Next Rule

b. Allow ICMP (including PING)

```
Menu 21.1.2 - TCP/IP Filter Rule

Filter #: 1,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 1     IP Source Route= No
^^^^^^^^^^^^^^^^
                Destination:        IP Addr= 0.0.0.0
                                    IP Mask= 0.0.0.0
                                    Port #= 0
                                    Port # Comp= None
                     Source:        IP Addr= 0.0.0.0
                                    IP Mask= 0.0.0.0
                                    Port #= 0
                                    Port # Comp= None
 TCP Estab= N/A
 More= No          Log= None
 Action Matched= Forward
             ^^^^^^^^
 Action Not Matched= Check Next Rule
```

c. Allow UDP traffic to ports > 1023

```
Menu 21.1.3 - TCP/IP Filter Rule

Filter #: 1,3
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17    IP Source Route= No
^^^^^^^^^^^^^^^^
                Destination:        IP Addr= 0.0.0.0
                                    IP Mask= 0.0.0.0
                                    Port #= 1023
                                          ^^^^
                                    Port # Comp= Greater
                                                 ^^^^^^^
                     Source:        IP Addr= 0.0.0.0
                                    IP Mask= 0.0.0.0
                                    Port #= 0
                                    Port # Comp= None
 TCP Estab= N/A
 More= No          Log= None
 Action Matched= Forward
             ^^^^^^^
 Action Not Matched= Check Next Rule
```

d. Allow TCP for ports > 1023, and drop all other packets.

```
Menu 21.1.4 - TCP/IP Filter Rule

Filter #: 1,4
Filter Type= TCP/IP Filter Rule
```

```
Active= Yes
IP Protocol= 6     IP Source Route= No
^^^^^^^^^^^^^^^^
            Destination:        IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 1023
                                      ^^^^
                                Port # Comp= Greater
                                           ^^^^^^^
               Source:          IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 0
                                Port # Comp= None
TCP Estab= No
More= No          Log= None
Action Matched= Forward
                ^^^^^^^
Action Not Matched= Drop  <== This is IMPORTANT!!
                  ^^^^
```

e. The Menu 21.1 will look like

Menu 21.1 - Filter Rules Summary

```
# A Type              Filter Rules                              M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP      Pr=0, SA=192.168.1.0, DA=0.0.0.0                    N F N
2 Y IP      Pr=1, SA=0.0.0.0, DA=0.0.0.0                        N F N
3 Y IP      Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP>1023              N F N
4 Y IP      Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP>1023               N F D
5 N
6 N
```

f. Plug it to Menu 11.1 Input Filter Sets.

g. If you have any server application running inside of your network, such as Domain Name Server, then you need to insert another filter before rule 4. For DNS, the filter rule will look like the following:

Menu 21.1.4 - TCP/IP Filter Rule

```
Filter #: 1,4
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17     IP Source Route= No
^^^^^^^^^^^^^^^^
            Destination:        IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 53
                                      ^^
                                Port # Comp= Equal
                                           ^^^^^
               Source:          IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 0
```

```
                                        Port # Comp= None
        TCP Estab= No
        More= No          Log= None
        Action Matched= Forward
                  ^^^^^^^
        Action Not Matched= Check Next Rule
```

h. The your Menu 21.1 will look like

Menu 21.1 - Filter Rules Summary

| # | A | Type | Filter Rules | M | m | n |
|---|---|---|---|---|---|---|
| 1 | Y | IP | Pr=0, SA=192.168.1.0, DA=0.0.0.0 | N | F | N |
| 2 | Y | IP | Pr=1, SA=0.0.0.0, DA=0.0.0.0 | N | F | N |
| 3 | Y | IP | Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP>1023 | N | F | N |
| 4 | Y | IP | Pr=17, SA=0.0.0.0, DP=53, DA=0.0.0.0 | N | F | N |
| 5 | Y | IP | Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP>1023 | N | F | D |
| 6 | N | | | | | |

i. Sometimes Internet application such as vedio conference need to use the UDP server port, then you have to be careful in setting up the firewall filter.

4. How do I configure the Router as a Remote Access Server?

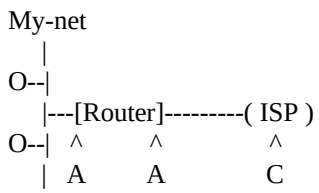
Configuring the Router is made simple by the SMT (System Management Terminal), a menu driven user interface. To configure the Router for use as a Remote Access Server, follow these steps.

4.a Windows 95 Remote User
Configure all the necessary parameters in Menu 13 for the Windows 95 Remote User. Then add a Remote User by configuring Menu 14. For a more detailed description of these Menus, please see the Router User's Manual.

4.b Other PPP Packages
The Router is compatible with many other PPP packages running in various platforms such as Windows 3.1x, Mac, Unix. Please check with D-Link on the compatibility list.

5. How do I configure my Router for my applications?

5.a Internet Access




The Router can allow multiple hosts on the LAN (My-net) to access the Internet through an ISP (Internet Service Provider). In this configuration, the Router is assigned a unique Ethernet IP address on ‘My-net’ (A). This address (A) will be also used to negotiate the connection with the ISP. Note that the IP address on ‘My-net’ are not hidden from the ISP and the rest of the Internet.

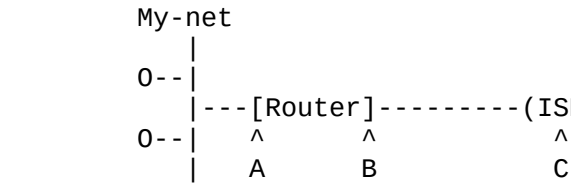
In Menu 1:
- Set **Route IP** to ‘Yes’.

In Menu 3.2:
- Set **IP Address** to an address on ‘My-net’ (A).

In Menu 4:
- Set **ISP IP Addr** to ‘C’.
- Make sure **Single User Account** is set to ‘No’.

In order for the nodes on ‘My-net’ to access the Internet, they need to have two items configured. First, the should set their ‘default gateway’ to the IP address of the Router (A). Second, they need to set their Domain Name Server address. If the LAN has a DNS present, use this address. Otherwise, you will have to obtain the DNS IP address from the ISP (not C).

5.b Internet Access with SUA




The Router allows multiple hosts on the LAN (My-net) to share a single IP address in the Internet. This address will be assigned by your ISP and is indicated in the above diagram by ‘B’. Note that the IP addresses on ‘My-net’ are hidden from the ISP and the rest of the Internet.

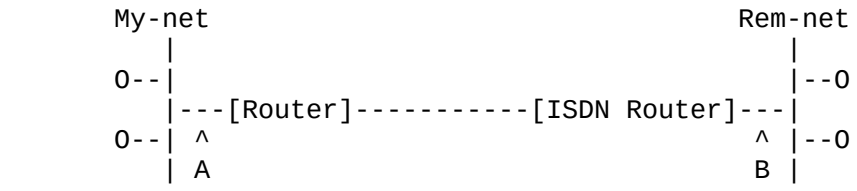
In Menu 1:
- Set **Route IP** to ‘Yes’.

In Menu 3.2:
- Set **IP Address** to an address on ‘My-net’ (A).

In Menu 4:
- Set **ISP IP Addr** to ‘C’.
- Set **Single User Account** to ‘Yes’.
- Set **Single User Account: IP Addr** to ‘B’. If the ISP assigns this address dynamically, leave this field blank or enter ‘0.0.0.0’
- Set **Single User Account: Server IP Addr** to the IP address of a server station on ‘My-net’. If the LAN has a Domain Name Server (DNS) station on it, the IP address of that station must be entered in this field (otherwise, this field is not required).

In order for the nodes on ‘My-net’ to access the Internet, they need to have two items configured. First, the should set their ‘default gateway’ to the LAN IP address of the Router (A). Second, they need to set their Domain Name Server address. If the LAN has a DNS present, use this address. Otherwise, you will have to obtain the DNS IP address from the ISP (not C).

5.c LAN to LAN for TCP/IP




The Router can allow multiple hosts on the LAN (My-net) to access a remote network's resources. In this configuration, the Router is assigned a unique Ethernet IP address on 'My-net' (A). Similarly, the remote ISDN router is issued a unique Ehternet IP address on 'Rem-net' (B). These addresses (A and B) will be also used to negotiate the connection between 'My-net' and 'Rem-net'.

In Menu 1:
- Set **Route IP** to 'Yes'.

In Menu 3.2:
- Set **IP Address** to an address on 'My-net' (A).

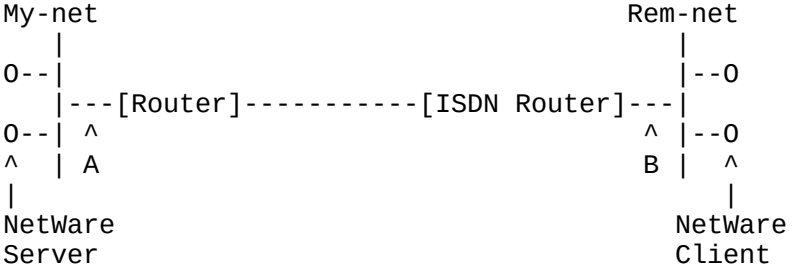
In Menu 11.1:
- Set **Route** to 'IP'.
- Set **Rem IP Addr** to the IP address of the remote ISDN router (B).
- Select 'Yes' to editing the IP options.

In Menu 11.3:
- Set **Rem Subnet Mask** to the subnet mask for the remote network.

The remote ISDN router (Cisco, Ascend...etc.) will have to complete similar configuration changes in order to talk to the Router.

5.d LAN to LAN for IPX

1. Router on the NetWare server side




The Router can accept calls from a remote router to negotiate IPX routing. In this configuration, the stations on the remote network (Rem-net) will have access to the IPX network resources available on 'My-net' and vice versa.

In Menu 1:
- Set **Route IPX** to ‘Yes’.

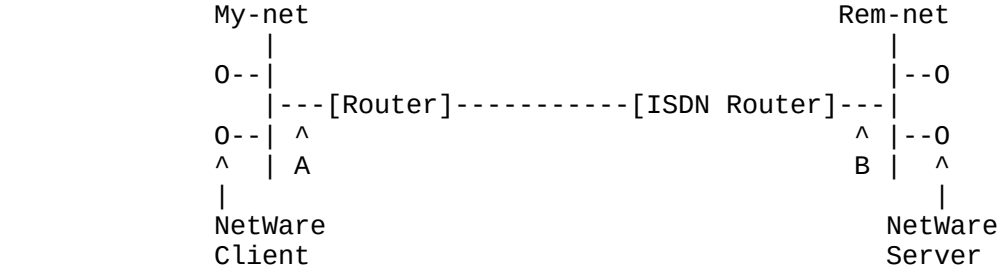
In Menu 3.3:
- Determine what frame type the client and server(s) stations are using and set the appropriate frame type to ‘Yes’. The Router will not be able to communicate with the nodes unless the frame types are the same.
- Set **Seed Router** to ‘No’. The Router will obtain the network numbers from the RIP broadcasts across the LAN.

In Menu 11.1:
- Set **Call Direction** to ‘Incoming’.
- Set **Route** to ‘IPX’, and select ‘Yes’ to editing the IPX options.

In Menu 11.3:
- Set **Dial-On-Query** to ‘No’.
- Set **Rem LAN Net #** to the external network number of the remote network (B).

The remote ISDN router (Cisco, Ascend...etc.) will have to complete similar configuration changes in order to talk to the Router.

2. Router on the NetWare client side




The Router can place calls to a remote ISDN router to negotiate IPX routing. In this configuration, the stations on the LAN (My-net) will have access to the IPX NetWare server and other network resources available on ‘Rem-net’ and vice versa. Note that in this setup, there is no NetWare server on ‘My-net’.

In Menu 1:
- Set **Route IPX** to ‘Yes’.

In Menu 3.3:
- Determine what frame type the client station(s) are using and set the appropriate frame type to ‘Yes’. The Router will not be able to communicate with the nodes unless the frame types are the same.
- Set **Seed Router** to ‘Yes’.

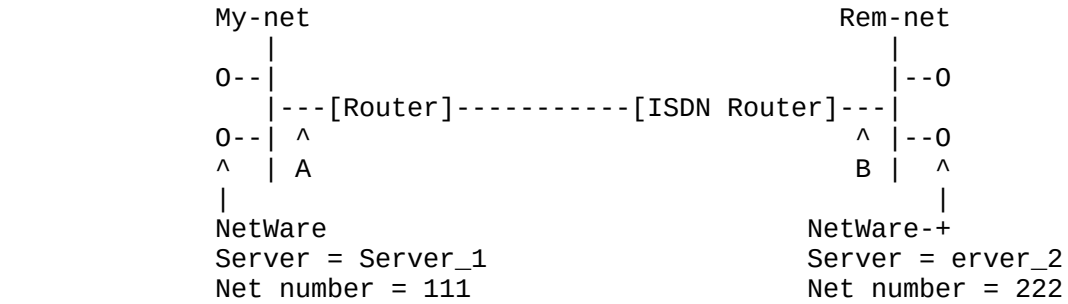
In Menu 11.1:

- Set **Call Direction** to ‘Outgoing’.
- Set **Route** to ‘IPX’, and select ‘Yes’ to editing the IPX options.

In Menu 11.3:
- Set **Dial-On-Query** to ‘Yes’.
- Set **Rem LAN Net** # to the internal network number of the remote NetWare server.

The remote ISDN router (Cisco, Ascend...etc.) will have to complete similar configuration changes in order to talk to the Router.

3. NetWare servers on both sides of the link




The Router can place calls to a remote ISDN router to negotiate IPX routing. In this configuration, the stations on the LAN (My-net) will have access to the IPX NetWare server on their own network. If the client stations on ‘My-net’ want to access the remote NetWare server (Server_2), then they will need to configure a static route for that Router.

In Menu 1:
- Set **Route IPX** to ‘Yes’.

In Menu 3.3:
- Determine what frame type the client station(s) are using and set the appropriate frame type to ‘Yes’. The Router will not be able to communicate with the nodes unless the frame types are the same.
- Set **Seed Router** to ‘No’.

In Menu 11.1:
- Set **Call Direction** to ‘Outgoing’.
- Set **Route** to ‘IPX’, and select ‘Yes’ to editing the IPX options.

In Menu 11.3:
- Set **Dial-On-Query** to ‘Yes’.
- Set **Rem LAN Net** # to the external network number of the remote network (B).

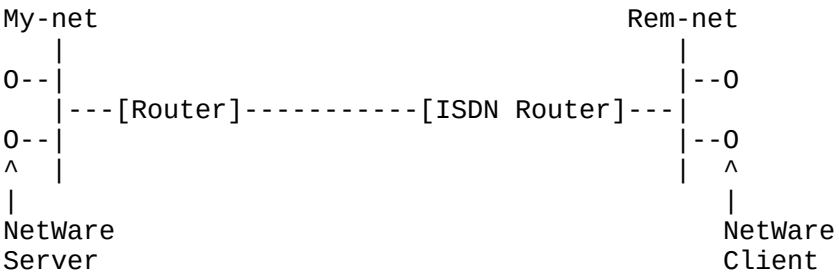
In Menu 12.2
- Set **Server Name** to ‘Server_2’ (The name configured for the server).

- Set **Active** to ‘Yes’.
- Set **Network** # to ‘00000222’ (The internal network number of the server).
- Set **Gateway Node** to the number of the remote node (1-4) for this setup.

The remote ISDN router (Cisco, Ascend...etc.) will have to complete similar configuration changes in order to talk to the Router.

5.e Bridging IPX

1. Router on the NetWare server side




The Router can accept calls from a remote router to Bridge IPX packets. In this configuration, the stations on the remote network (Rem-net) will have access to the IPX network resources available on ‘My-net’.

In Menu 1:
- Set **Bridge** to ‘Yes’.

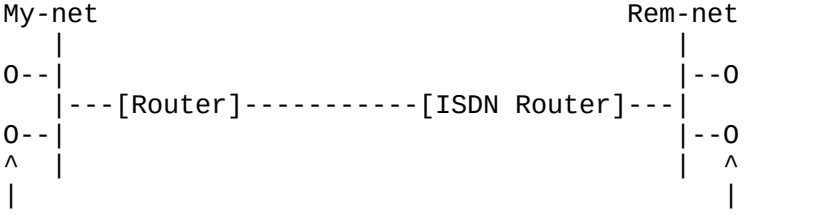
In Menu 3.4:
- Set **Handle IPX** to ‘Server’.

In Menu 11.1:
- Set **Call Direction** to ‘Incoming’.
- Set **Bridge** to ‘Yes’.
- Select ‘Yes’ to editing the Bridge options.

In Menu 11.3:
- Set **Dial-On-Broadcast** to ‘No’.

The remote ISDN router (Cisco, Ascend...etc.) will have to complete similar configuration changes in order to talk to the Router.

2. Router on the NetWare client side



```
      NetWare                                   NetWare
      Client                                    Server
```

The Router can place calls to a remote ISDN router to Bridge IPX packets. In this configuration, the stations on the LAN (My-net) will have access to the IPX NetWare server and other network resources available on 'Rem-net'. Note that in this setup, there is no NetWare server on 'My-net'.

In Menu 1:
- Set **Bridge** to 'Yes'.

In Menu 3.4:
- Set **Handle IPX** to 'Client'.

In Menu 11.1:
- Set **Call Direction** to 'Outgoing'.
- Set **Bridge** to 'Yes'.
- Select 'Yes' to editing the Bridge options.

In Menu 11.3:
- Set **Dial-On-Broadcast** to 'Yes'.

The remote ISDN router (Cisco, Ascend...etc.) will have to complete similar configuration changes in order to talk to the Router.

5.f Windows 95/NT Dialing in for TCP/IP

```
      My-net
         |
      O--|
         |---[Router]---------[ISDN TA]---O
      O--|   ^      ^         ^           ^
         |   A      A         C       Win 95/NT
```

The Router can accept calls from a remote station equipped with remote access software (such as Windows 95 Dial-Up Networking). The remote station uses an ISDN terminal adapter to make the connection. In this configuration, the remote station will have access to the TCP/IP network resources available on 'My-net'. There are two ways to set the IP address for the remote station (C). This can be set statically set by the remote station, or it can be dynamically set by the Router.

In Menu 1:
- Set **Route IP** to 'Yes'.

In Menu 3.2:
- Set **IP Address** to an address on 'My-net' (A).

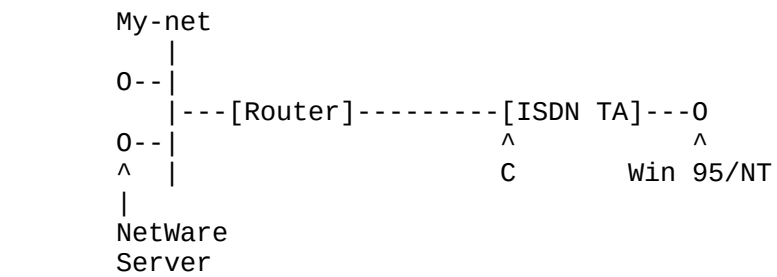
In Menu 13:
- Set **Recv Authen.** to PAP.
- Set **Dial-in User** to 'Yes' if the remote station will provide its own IP address (C). Otherwise, set to 'No'.
- Set **IP Pool** to 'Yes' if you want the Router to assign an IP address to the remote station.

If you are using the **IP Pool**:

- Set **IP Start Addr** as IP address assigned to the remote station (C).
- Set **IP Count(1,2)** to be the number of IP addresses in the pool.

In Menu 14.1:
- Set **User Name** to be the login name for the remote station.
- Set **Passwd** to be the password for the remote station.

5.g Windows 95/NT Dialing in for IPX




The Router can accept calls from a remote station equipped with remote access software (such as Windows 95 Dial-Up Networking). The remote station uses an ISDN terminal adapter to make the connection. In this configuration, the remote station will have access to the IPX network resources available on 'My-net'. There are two ways to set the external network number for the remote station. It can be set provided by the Router from a pool, or it can be generated randomly.

In Menu 1:
- Set **Route IPX** to 'Yes'.

In Menu 3.3:
- Determine what frame type the client and server(s) stations are using and set the appropriate frame type to 'Yes'. The Router will not be able to communicate with the nodes unless the frame types are the same.
- Set **Seed Router** to 'No'. The Router will obtain the network numbers from the RIP broadcasts across the LAN.

In Menu 13:
- Set **IPX Pool** to 'Yes' if you want the Router to assign a pre-configured IPX network number to the remote station. Otherwise, the Router will generate a random network number for the remote station.

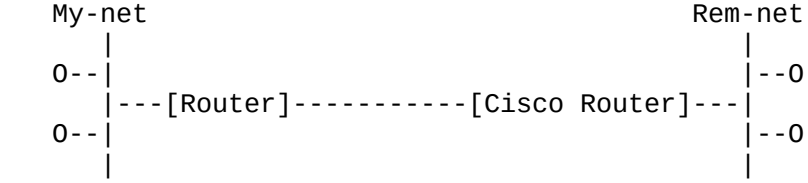
If you are using the **IPX Pool**:

- Set **IPX Start Net Num.** as the starting IPX network number you wish to assign to the remote station (C).
- Set **IPX Count(1,16)** to be the number of IPX network numbers in the pool.

In Menu 14.1:
- Set **User Name** to be the login name for the remote station.
- Set **Passwd** to be the password for the remote station.

6. How do I configure my Router to work with other devices?

Cisco Router




Due to Cisco's authentication scheme, you need to configure some additional fields when talking to a Cisco device. There are two instances to pay attention to. The first is Cisco's mutual authentication scheme, and the second is their interpretation of CHAP.

If the Cisco router requests PAP:
In Menu 13:
- Set **Mutual Authen** to 'Yes'.
- Set **PAP Login** to the appropriate login name.
- Set **PAP Password** to the appropriate login password.

If the Cisco router requests CHAP:

Note: The Cisco device must be configured as a remote node and not a remote user.

In Menu 11.1 (only if **Call Direction** is 'Incoming' or 'Both'):
- Set **Incoming: Rem Login** to the Cisco device hostname.
- Set **Outgoing: My Login** to the **System Name** value in menu 1.
- Set **Incoming: Rem Password** to be the same as **Outgoing: My Password**.

7. How can I protect against IP spoofing attacks?

The Router's filter sets provide a means to protect against IP spoofing attacks. The basic scheme is as follows:

For the incoming data filters:
- Deny packets from the outside that claim to be from the inside
- Allow everything that isn't spoofing us

Filter Type= TCP/IP Filter Rule
Active= Yes
Source: IP Addr= a.b.c.d
Source: IP Mask= w.x.y.z
Action Matched= Drop
Action Not Matched= Forward

where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask

For the outgoing data filters:
- Deny "bounceback" packets
- Allow packets that originate from us

Filter Type= TCP/IP Filter Rule
Active= Yes
Destination: IP Addr= a.b.c.d
Destination: IP Mask= w.x.y.z
Action Matched= Drop
Action Not Matched= Forward

where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask

8. I want to assign an IP address to my workstation dynamically...how?

The Router can assign IP addresses during the IPCP negotiation, but that only applies to the device that's calling in, either a remote router or a remote workstation with a TA. The Router cannot assign IP addresses to any workstations behind the router, because nothing on that workstation performing the IPCP negotiation.

In the case of a workstation calling in using an ISDN TA, the Router is able to assign the IP address because it is the workstation that is doing the actual PPP/IPCP negotiation.

9. How can I prevent incoming telnet sessions to my Router?

The Router has implemented a telnet password, which must be entered before a telnet session is established. This password is the same as the system password configured in menu 23. In addition, the Router will only allow one administrator to configure the device at a time. Any attempted telnet session will be rejected if an administrator is already logged into the SMT.

If you want to block all incoming telnet sessions from being established, you can define an IP filter and plug it into the incoming data filters for appropriate remote connection:

Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6
Destination: IP Addr= w.x.y.z
Destination: IP Mask= 255.255.255.255
Destination: Port #= 23
Destination: Port # Comp= Equal
Action Matched= Drop
Action Not Matched= Forward

where w.x.y.z is the IP address of your Router.

10. How can I backup/restore my configuration remotely?

Currently, the only method available for backing up and restoring the Router's configuration is locally through the RS-232 port. Menu 24.5 and 24.6 provide simple methods to perform the backup and restoration.

11. How do I enable DOVBS when I make an outcall?

You can enable DOVBS (Data Over Voice Barrier Service) can be enabled in menu 11. When you configure your remote node to make an outcall, set the 'Telco Option: Transfer Rate' field to 'DOVBS'. If you check the system status menu (24.1) the connection Type should be 56K.

The Router can automatically detect an incoming DOVBS call. Once the call is connected, menu 24.1 will also indicate a Type of 56K.

12. How I can prevent any packets from triggering a call?

For those customers that pay by the call, and not the minute, they can set up a call filter to stop packets from triggering the call. Set the destination IP address to 0.0.0.0 (filter ALL packets). Also set the Idle Timeout of that remote node to zero. To trigger the call in this scenario, use the option in menu 24.4.5 (manual call). This way, the call will never time out but it will also never automatically dial either.

13. How can I turn on call tracing tools?

For call setup EPA trace:
. Go to CI (Menu 24.8) issue 'isdn ana on' command
. make a call
. after the call failed (disconnected), issue 'isdn ana off' and 'isdn ana disp' (You have to do this in RS-232 connection, and use the PgDn in number keypad to scroll the trace)

For PPP trace:
. Go to CI, 'sys trcl cl' and then 'sys trcl sw on', 'sys trcp sw on'
. make a call
. 'sys trcl disp' to display the traces

14. How can I configure the correct default static route for my Router?

You can do this by configuring an IP static route in menu 12. The Destination IP Address for this route should be '0.0.0.0'. Once this has been configured, the default route should be stored correctly.

15. How do I setup the Router to make MP calls?

By default, the Router is set to only make single link calls (using 1 B-channel). You can configure your Router to make an MP call by setting some parameters for that Remote Node. When you

get to the Remote Node configuration screen, select 'Yes' to Edit the PPP options. There are two ways to setup the MP call:

a. Set Base Trans Rate to '128'. This will bring up both channels every time the call is placed.

b. Set Base Trans Rate to '64' and Max Trans Rate to '128'. This will bring up the second B-channel based on the traffic across the link. Please see the manual for more information.

16. How do I block Win95 or NT's NetBEUI over IP packets from triggering a call to my ISP?

Setup a filter set as follows, and plug it in Menu 11 for the ISP remote node in the 'Call filter sets='.

```
                        Menu 21.1 - Filter Rules Summary
# A Type                   Filter Rules                        M m n
- - ---- ------------------------------------------------- - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=138, DA=0.0.0.0              N D N
2 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0              N D F
3 Y IP   Pr=6, SA=0.0.0.0, SP=138, DA=0.0.0.0               N D N
4 Y IP   Pr=6, SA=0.0.0.0, SP=137, DA=0.0.0.0               N D F
5 N
6 N
```

```
                    Menu 21.1.1 - TCP/IP Filter Rule

                    Filter #: 1,1
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                IP Protocol=        17   IP Source Route= No
                Destination:        IP Addr= 0.0.0.0
                                    IP Mask= 0.0.0.0
                                    Port #= 0
                                    Port # Comp= None
                    Source:         IP Addr= 0.0.0.0
                                    IP Mask= 0.0.0.0
                                    Port #= 138
                                    Port # Comp= Equal
            TCP Estab= N/A
            More= No        Log= None
            Action Matched= Drop
            Action Not Matched= Check Next Rule


            Menu 21.1.2 - TCP/IP Filter Rule

            Filter #: 1,2
            Filter Type= TCP/IP Filter Rule
            Active= Yes
                IP Protocol=        17   IP Source Route= No
                Destination:        IP Addr= 0.0.0.0
                                    IP Mask= 0.0.0.0
                                    Port #= 0
                                    Port # Comp= None
```

Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 137
Port # Comp= Equal
TCP Estab= N/A
More= No Log= None
Action Matched= Drop
Action Not Matched= Forward

Menu 21.1.2 - TCP/IP Filter Rule

Filter #: 1,3
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6 IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 0
Port # Comp= None
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 138
Port # Comp= Equal
TCP Estab= N/A
More= No Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule

Menu 21.1.2 - TCP/IP Filter Rule

Filter #: 1,4
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6 IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 0
Port # Comp= None
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 137
Port # Comp= Equal
TCP Estab= N/A
More= No Log= None
Action Matched= Drop
Action Not Matched= Forward

## Part III: Troubleshooting Questions

1. My connection won't stay down. How can I prevent this?

The Router comes with several pre-defined call filters designed

to prevent certain IPX packets from triggering a call to a remote node. These filters should inform your Router which packets should be ignored as traffic.

If you are routing IPX packets, the default call filters are defined as follows:

- Block periodical SAP and RIP response messages
- Block NetWare serialization packets
- Allow SAP and RIP enquery packets

If you are bridging IPX packets, the default call filters are defined as follows:

- Block periodical SAP and RIP response messages
- Block SAP and RIP enquery packets if set to Handle IPX as 'Server'
- Allow SAP and RIP enquery packets if set to Handle IPX as 'Client' or 'None'

If you want to prevent packets from other protocols from triggering the call, you can block an entire protocol type by setting up a generic filter rule in the following way:

Filter Type= Generic Filter Rule
Active= Yes
Offset= 12
Length= 2
Mask= ffff
Value= [protocol ID]
More= No
Action Matched= Drop
Action Not Matched= Forward

If your filtering scheme requires you to block more specific packets, you can determine the type of packet that is triggering your call by looking in menu 24.1. First drop your connection, and then stop all data traffic. The line should stay idle. If the call is still triggered, then you can check menu 24.1, and by looking at the packet format, you can adjust your filter set accordingly to block these packets.

2. Why does the Router still drop the call after the authentication has passed?

In some cases, when you are negotiating a connection, you may notice that the call will be dropped even though the CHAP or PAP authentication phase was successful. The reason for this may be because the IPCP negotiation has failed due to an IP address mismatch. The Router uses the IP address as another form of authentication, so if the address supplied by the remote node does not match the address the Router is expecting, the call will be dropped.

3. Why does my screen keep blanking out?

In both an RS-232 connection and a telnet session, the SMT

(System Management Terminal) has a system timeout of five minutes. That is, if you do not perform a keyboard operation in five minutes then the screen will blank out or your telnet connection will be dropped. You can disable this timeout by going into CI mode, and typing the command: sys stdio 0

4. Will my screen blank out if I stay in menu 24.1?

No. If you keep your system on menu 24.1, the system will not timeout after the five minutes has elapsed.

5. What can I do if I don't know the IP address of the device I am connecting to?

In some cases, your Internet Service Provider (ISP) or other remote node you wish to connect to will not know their IP address.

You can work around this problem by using the Internet Setup Menu (menu 4) to configure your remote node. In this screen, you have the option to leave the ISP's IP address field blank or simply enter 0.0.0.0. In these cases, the Router will accept any IP address sent from that device.

If you want the remote device to dynamically assign an IP to the Router, then you need to turn on the Single User Account feature, and leave the IP Addr field blank or filled with 0.0.0.0.

6. Why do I see garbage characters being printed out on my console?

This condition is due to data overflowing the UART. You may not have a 16650 UART chip on your serial port, or you might not have flow control working correctly on that port. There is no harm caused by this data overflow. You can repaint the screen by escaping back one menu and then re-entering the screen.

7. My Router inexplicably reboots itself. Why?

The could be a problem with the power supply connection on the rear panel of the Router. The connection may be loose and causing the Router to reboot itself. When you plug in the power cable, make sure that you apply the force behind the sliding collar and not holding it. This will ensure a good connection. To test if the connection is firm, hold the back of the power cable plug, just behind the sliding collar, and try pulling the cable out. If the connection is firm, you should not be able to pull the cable out without pulling the sliding collar back.

8. Why can't I get the callback feature to work when I dial from a workstation to the Router?

Router only supports Microsoft's proprietary CallBack Control Protocol (CBCP). Thus, the Router will only be able to do PPP callback to other devices that also support CBCP, such as Win95 or NT. If you are using Trumpet or other application that doesn't support CBCP, Router will not callback.

9. Dial-in users to the Router cannot talk to some or all of the stations on the LAN side of Router, or access Internet through another router on the LAN (Dial-in user are using IP address in IP pool) Why?

   The reason for this is very simple, the stations on the LAN side of Router do not have a route back to Remote dial-in user. To fix this:

   A. If you can turn on RIP to 'both' in Menu3.2, then Router will send out RIP for the route to the dial-in user. For other routers or workstations on the LAN that can accept the RIP, they will have a route to the remote dial-in user.
   B. For stations that cannot turned on RIP or does not support RIP, then you need to add a static route for the IP addresses in the Router IP pool, which is the IP address for the remote dial-in user. For example, if local workstation is a Win95 station, then you need to add the static route as:
      Win95> route add a.a.a.a MASK 255.255.255.255 p.p.p.p
   C. Subneting your network, and assign one subnet to internal LAN. Use the IP address in another subnet for the IP pool. However, you still need to have RIP turned on.

10. How do I trace if my Router is doing callback on CLID?

    1. Set Menu 13 CLID authentication to 'Required'
    2. Go to Menu24.8 (CI) and type 'sys event'
    3. Make a call from the remote side

    All events such as incoming call, callback traces will show up on the screen

11. My RS232 connection to Router can't access Router. Why?

    Besides the speed, COM port, RS232 cable, there's one more thing to check the serial card in your PC. If you use a D-Link double or quad speed serial port (which I use with the IU unit), then whatever you select the speed in your Terminal Emulation program will be time 2 or 4 to communication to Router.

**Part IV: Feature Description Questions**

1. What is the Single User Account (SUA) Internet Access and should I use it?

   Most Internet Service Providers (ISP) offer two types of service: a Class C address account or a single user account. A Class C address account allows a company with up to 255 workstations to access Internet concurrently, while a single user account only allows one user to access Internet. The service charges for a Class C address account is typically much higher than that for a single user account.

   The Router has a unique feature called Internet Single User Account (SUA) which allows multiple people to access Internet

concurrently for the cost of a single user.

NAT is a generic name defined in RFC 1631 "The IP Network Address Translator (NAT)". SUA (Internet Single User Account) is D-Link's
implementation and trade name for this functionality.

The primary motivation for RFC 1631 is that there are not enough IP addresses to go around. In addition, a great many corporations simply did not bother to obtain legal (globally unique) IP addresses for their networks and now finding themselves unable to connect to the Internet.

Basically, NAT is a process of translating one address to another. An NAT implementation can be as simple as substituting an IP address with another. This allows a network to rectify the illegal address problem mentioned above without going through each and every host.

The design goal of D-Link's SUA is to minimize the Internet access cost in a small office environment by using a single IP address to represent the multiple hosts inside. It does more than IP address translation, so that multiple hosts on the LAN can access the Internet at the same time.

The legal gateway IP address can be statically assigned or the Router can dynamically ask the ISP for it. The number of simultaneous users is limited by the fixed-size translation table; a reasonable number being less than 20 users. Beyond that, the single ISDN pipe would probably become the bottleneck and any increase in the translation table size will not help.

SUA is an ideal solution for a small office environment with less than 20 people and one server. For more than 20 people or more than one server, a Class C address is recommended.

2. Can I setup two SUA account?

No, SUA account can only be setup in Menu 4, therefore, you cannot setup two SUA account. If you set 0.0.0.0 or don't set any IP address in Menu 11 for the 'Rem IP Addr', Router will not allow you to save it.

3. Can I use a phone and the Router on the same BRI?

3.a Analog (POTS) phone
The Router has a built-in standard phone jack (POTS) which means that you can use any analog device (phone, answering machine, fax machine, etc.) on the same BRI.

4. How do I set up the Router to use the POTS port?

Plug your analog device (phone, answering machine, fax maching, etc.) into the POTS port of your Router. Then make sure in menu 2 that one of the phone numbers 'Analog Call' field is set to 'Voice'. You can then make and receive calls from your device

with that phone number.

5. How do I use the Syslog feature to account for my calls?

The Router can be configured to send UNIX syslogs to a host on the LAN that runs a syslog daemon (most UNIX systems will do). This feature can be configured in menu 24.3.2:

- Active= Yes
- Syslog IP Address= [IP address of logging host]
- Log Facility= localn

where ‘n’ is a number from 0 to 7.

You can use this feature to handle your call accounting because the Router will send out Call Information Syslog messages detailing incoming and outgoing calls. The format of these messages are as follows:

- [timestamp] line 1 channel 1, call 41, C01, Incoming Call, 40001
- [timestamp] line 1 channel 1, call 41, C01, ANSWER Connected, 64K 40001
- [timestamp] line 1 channel 1, call 41, C01, Incoming Call, Call Terminated

6. How do I setup syslogd in UNIX to use Router build-in log capability?

Here are some examples of different ways to setup the syslog daemon configuration file to take the log:

```
<example 1>
/etc/syslog.conf:
local1.info            /var/log/D-Link_log_1
local2.info            /var/log/D-Link_log_2
```

Go to /var/log create D-Link_log_1 and D-Link_log_2 by 'touch D-Link_log_1' and 'touch D-Link_log_2'. In Router, if you set the 'Log Facility' to 'local1', then the log will be log to file D-Link_log_1. If you set to 'local2', the log will go to file D-Link_lo_2.

```
<exampel 2>

/etc/syslog.conf:
*.info                 /var/log/D-Link_log
```

Create D-Link in /var/log directory.

```
<example 3>
local0.*               /usr/adm/D-Link.log
local1.*               /usr/adm/D-Link.log
local2.*               /usr/adm/D-Link.log
*.=info;*.=notice      /usr/adm/messages
```

Note: In the configuration file:

1) Put the most restrictive things at the front. This syslog.conf will get everything from local 0,1,2, no matter what level it is, and send it to D-Link_log
2) USE TABS!!!! No spaces!

7. What are the debugging commands for the Router? Can I debug my problems?

Debugging problems on the Router can be an extremely involved process. We recommend that you follow the general procedure for some common problems defined below.

7.a ISDN initialization failed

Check the error log (menu 24.3.1), and look for 'ISDN init failed. code<X>'.

If 'X' = 1: This means that the link is not up. A possible reason is that the ISDN line is not active or not connected to the Router properly.

If 'X' = 2: This refers to a SPID error. Check the SPIDs entered in menu 2 and try again.

If 'X' is any other code, then check the ISDN switch type you have configured in menu 2, as well as the country code in menu 24.1. If these are correct, then you need to turn on the protocol analyzer to analyze the ISDN traces. To do this, you need to be connected to the Router via the RS-232 cable with the terminal mode set to ANSI. To scroll the screen, you can use the PgUP and PgDn keys.

Go to CI (menu 24.8)
> isdn ana on
> isdn init
> isdn ana off
> isdn ana disp

7.b Can't connect to the Internet/remote node

After you have configured menu 4, go to menu 11 and check which remote node is used for this '(ISP)', for example, let's say it is number 1.

Go to menu 24.4 and select 'Manual Call', and select 1 as the Remote Node. You should be able to see the traces for the connection setup process.

If you are familiar with the PPP negotiation, you can turn on the PPP tracing mechanism while you start an outcall to the remote node in question.

Go to CI (menu 24.8)
> sys trcl cl
> sys trcl sw on
> sys trcp sw on

> ip ping a.b.c.d (where a.b.c.d is the remote gateway IP address)
(after the call stops)
> sys trcl disp

You will see the tracelog as well as the packet traces.

7.c Can't PING to or from the LAN on the Router

First check your physical LAN connection by checking the LAN LED on the front panel; this should be on. Also check the other end of this connection (to the hub).

Go to menu 3.2 and check that the Router is on the same network/subnet as the other stations on the network.

Go to CI (menu 24.8)
> ip route stat
> ip ping w.x.y.z (where w.x.y.z is another station on the network)
> ip route stat

By examining the routing table before and after the PING, you should note that the 'Use' field for that route should have been incremented by 3.

If not, then use
> ip route errcnt disp
to determine the cause.

If it has been incremented, then try
> lan cnt disp
to check if there is a hardware problem.

Finally, check for any filter sets that may have been implemented that could prevent the PING packet from going through.

7.d Workstations on the backbone LAN cannot access the remote node

Check that the Router has been connected to that remote node; use menu 24.5 'Manual Call'. Try to PING from the Router to the remote node.

Verify the LAN connection by trying to PING from the workstation to the Router or vice versa.

If you want the Router to make a call every time the workstation tries to send a packet to that remote node, check that the Call Direction field is set to 'Outgoing' in menu 11.

Try to PING from the workstation to the remote node. This should trigger the outcall.

If it does not trigger the outcall, check to see if there are any filters blocking the packet.

Go to CI (menu 24.8) and check the routing table

> ip route stat
The ‘Use’ for the route to that remote node should have been incremented. If it hasn’t then examine the routing table to determine why.

Check whether the call has been triggered by using
> dial cnt disp

8. Does the Router support CLID (Calling Line ID) authentication?

Yes, the Router can authenticate an incoming call based on the CLID. To enable this feautre simply enter the CLID value into the appropriate field in either the remote node menu or the remote user menu. Then in menu 13, you can set the ‘CLID Authen=‘ field to one of three options.

- None - will not authenticate the incoming call’s CLID
- Required - authenticates solely on the basis of the incoming call’s CLID
- Preferred - checks the incoming calls CLID. If successful, no further authentication is done. If unsuccessful, the Router will attempt the requested PPP authentication (CHAP or PAP).

9. Does the Router support SNMP?

The Router implements an SNMP 'agent' which provides networking information to the SNMP 'manager' applications running on other computers. In addition to supporting the objects defined in the standard RFC MIBs, the Router also supports objects defined in the D-Link-specific MIB which can be found in D-Link’s ftp site.

10. How do I use Menu 24.1 in the SMT?

Menu 24.1 displays some very useful sytem status information. This System Status screen is a tool that can be used to monitor your Router. Specifically, it will give you information on the status of your system software version, ISDN telephone link status, total outcall time, number of packets sent, number of packets received, and other useful status information.

There are three basic commands you can use in Menu 24.1. These are:

1. Drop the current B1 channel call.
2. Drop the current B2 channel call.
3. Reset the counters.
4. Drop all calls.

11. Why is the default password, ‘1234’, rejected when I first power on my Router?

Your communications program may be set up incorrectly. The communications program needs to support vt100 terminal emulation with the parameters set to 8N1 (8 data bits, non-parity, and 1 stop bit).

12. How does the Router assign its calling party ID numbers for outgoing calls?

    The Router assigns these numbers based on the phone numbers you enter in menu 2.

13. Can you clarify the capabilities of the Router for using both B-channels simultaneously?

    The Router can simultaneously do the following:

    Make 2 ISDN data calls (either bundled or to separate nodes).

    Make 1 ISDN data call and 1 POTS or A/B adapter (voice) call.

14. If I want to monitor line status in Menu24.1, will it auto-logout after 5 minutes?

    No, the SMT will not timeout in Menu 24.1.

15. Can I use Router CLID callback feature to callback to Windows 95 or Windows NT?

    No, you can’t. The reason is Win95 and NT must use CBCP to negotiation the callback function. If you use the CLID callback, Router will do a callback without answering the incoming call. To Win95, this is a call failure, and Win95 will not reach to a state to wait for callback.

16. Can I use the Router CLID callback feature to call back to a remote node?

    Yes, you can configure CLID callback to a remote node by setting the following parameters:

    . the CLID Authen field in menu 13 must be set to ‘Required’
    . the Remote Node call direction must be set to ‘Both’
    . the Remote Node must have enabled the CLID service on their ISDN
    . the CLID must match the value you give in the ‘Rem CLID’ field
    . the number entered in 'PrI Phone #' will be the number dialed

17. Can I manually set the CLID callback timer?

    Yes, you can set the delay time before Router starts a CLID callback. The default value is 5 seconds, and you can change it in SMT 24.8 (CI) by issuing ‘dial timeout callback <seconds>’.

18. How do I drop both B channels when they are bundled in an MP call?

    You can go to Menu 24.8 and issue ‘isdn drop all’ to drop both B channels.

19. What do CLU and ALU mean in Menu 24.1? What's the relationship to MP/BOD?

CLU is the current line utilization. It's the percentage of the total bandwidth being used.

ALU is the average line utilization. It's the percentage of the average bandwidth used.

The calculation of these values depends on rather the link is to a remote node or dial in user. If the link is to a remote node, it depends on what is choose in Menu 11.2, Remote Node PPP Option, for BOD Calculation. If the choose is Receive, then CLU and ALU represent only the incoming traffic. If the choose is Transmit, then they represent only the outgoing traffic. If the choose is Transmit or Receive, then it represents whichever traffic is greater. Dial in user links always calculate as Transmit or Receive.

Why is remote node calculation so complicated?
Because it's also used for bringing up the second channel.
So, if you set you Target Utility as 32-48Kbps and the connection speed is 64K, then the second line will be brought up if the CLU reaches 75% and the second line will be dropped if CLU drops to 50%. ( Note, the CLU has to maintain that level of usage for the specified persist time before the second line is brought up or dropped. )

20. How do I setup Compression to work with Ascend?

Ascend supports 2 styles of Stac compression. One is their proprietary stuff that was implemented before CCP standard was finalized. For unknown reasons, they did not request it to be included in the standard. The other is what they call "MS-Stac", which is actually check mode 4 in the standard. D-Link does not support their proprietary check mode. We support check mode 3 (sequence number) and 4 (extended mode, proposed by Microsoft) in the standard.

If CCP negotiation fails, it could be 1. compression is off; or 2. compression is set to "Stac", instead of "MS Stac" in Ascend MAX/Pipeline.

**Part V: Miscellaneous Questions**

1. How can I tell what version of system code I have?

For the RAS software version: see menu 24.1
For the ISDN firmware version: see menu 24.1
For the bootmodule version: see the screen during system startup

2. How can I upgrade system code?

The SMT (System Management Terminal) has an option (Menu 24, option 7) that allows you to easily upgrade the system code. Once you execute this option, you can follow the onscreen instructions to upload the system code. You will need to invoke XMODEM to download the code. For a more detailed description of

this procedure, please refer to: Maintenance of the User's Guide.

3. What can I do if I have problems upgrading my system code?

   If you have any problems when you upload the system code, try uploading the code in a DOS environment as opposed to a Windows environment.

4. How can I get the Novell NetWare server's internal network number?

   The easiest way to obtain the NetWare server's internal network number is to ask the system administrator. If this option is unavailable, then you can attempt to find this value in the following way:

   - Connect a Router to the same LAN as the NetWare server
   - In the Router, go to menu 24.8 (Command Interpreter mode)
   - Check the internal SAP information by issuing the command, 'ipx sap status'
   - You should be able to see the network number for the corresponding server

5. Should I use routing or bridging between two Routers?

   The answer to this question depends on the situation and the type of network in question. Generally, routing provides better security, better prevention of unneeded traffic, and more flexibility. However, bridging provides the advantage of conserving IP address space. So if you have many stations, but only limited addresses, it may be a better option to bridge.

6. What do the 'M m n' mean in 21.1?

   M: refers to 'More' filter rules. 'Y' means don't do any action and check the next rule.
   m: refers to 'match'. Actions can be Forward, Drop, Next-rule.
   n: refers to 'not match'. Actions are the same as above.
   (Please refer to page 11-3 in manual for more details).

7. How can I set the country code for my Router?

   The country code (displayed in menu 24.1) can be changed using a CI command. First go to command mode (menu 24.8). The command 'sys countrycode <code>' will change the country code. <code> refers to the country code in decimal. For instance, 'sys countrycode 255' will set the Router to a North American country code.

   The country code will also be displayed using the debug command 'atsh'. However, this value is for manufacturer use only, and so only the default country code will be displayed here.