

Prestige 480

Dual BRI ISDN Router

User's Guide Supplement

Mega Bundle or Multiple ISPs Support

IP Alias

NetCAPI

RADIUS Accounting

Multiprotocol Support (IPX Routing and Bridging)

Backup and Restore Configuration File using FTP

Firmware and Configuration Files Upload using FTP

IP Policy Routing

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

Mega Bundle or Multiple ISPs Support

Basics

If ISPs do not support multilink bundle of more than 2 links, it would be impossible for a user to dedicate all 4 channels available in a P 480 to Internet access. To differentiate P 480 from other similarly equipped products, it is desirable to be able to support bundle of 4 links where P 480 calls a second ISP when the traffic exceeds a certain threshold and split the traffic between the two connections. The Prestige refers to this multiple ISPs support as Mega Bundle.

Mega Bundle design is as listed below.

1. *One remote node* is designated as the main ISP and *another* the supplementary ISP. The Prestige dials the first and second link on the main ISP using the existing mechanism.
2. If a supplementary remote node is specified, BOD behaves as if the maximum number of channels is 4 and the adding and dropping of channels are governed by the main remote node's multilink parameters alone.
3. When the traffic triggers the third link (as determined by BOD), the Prestige calls the supplementary ISP. Since the new connection is a separate PPP session, it will have a different IP address and thus a new interface.
4. Because of NAT, if an IP connection is already assigned to a particular interface, then it must remain on that interface. For new connections, the round-robin method is used to assign a connection to either the main or the supplementary ISP. Non-IP traffic is simply distributed evenly on a packet-by-packet basis.
5. Once the Prestige determines which interface a connection uses, the MP channel assignment within each bundle remains the same as the existing method.

ISP Remote Node and Supplementary Remote Node

The previous ZyNOS versions supported only one ISP account. That remote node is called as the “ISP remote node”. Now in ZyNOS v2.42, you can setup other ISP accounts and this is called as “supplementary remote node”.

You can have several “Supplementary remote node”, but only one “ISP remote node”. These remote nodes can work at the same time. “Supplementary remote” is almost the same as “ISP remote node” except that “supplementary remote node” will not appear in the routing table as default route.

Configuring Mega Bundle

Step 1. Configure an ISP remote node.

1. Setup ISP in **Menu 4**.
2. Set **Multilink= BOD** or **Multilink= Always** in **Menu 4**

```
Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No
BACP= Enable
Mega Bundle= None

Multiple Link Options:
  BOD Calculation= Transmit or Receive
  Min. Channels= 1
  Max. Channels= 1
```

Figure 1 Remote Node PPP Options

3. In **Menu 11**, edit the ISP remote node.
4. Set **Edit PPP Options= Yes** and then press [Enter]. You will enter **Menu 11.2**
5. In **Menu 11.2**, set **Max. Channels= 3** or **Max. Channels= 4**
6. Save the configuration.

Step 2. Configure a supplementary remote node.

1. Setup a remote node in **Menu 11**.
2. Set **Edit PPP Options= Yes** and then press [Enter]. You will enter **Menu 11.2**
3. Set **Mega Bundle= Supplementary**. Return to **Menu 11.1**.
4. Set **Rem IP Addr= 1.2.3.4**. The value can be arbitrary IP address except **0.0.0.0** and **1.1.1.1**.
5. Set **Edit IP/IPX/Bridge= Yes** and then press [Enter]. You will enter **Menu 11.3**.
6. Set **Rem Subnet Mask= 0.0.0.0**
7. Save the configuration.

Check the configuration in **Menu 11**. If the supplementary remote node is configured, you can see it in **Menu 11**. The following is a reference screen. Node 2 is a supplementary remote node.

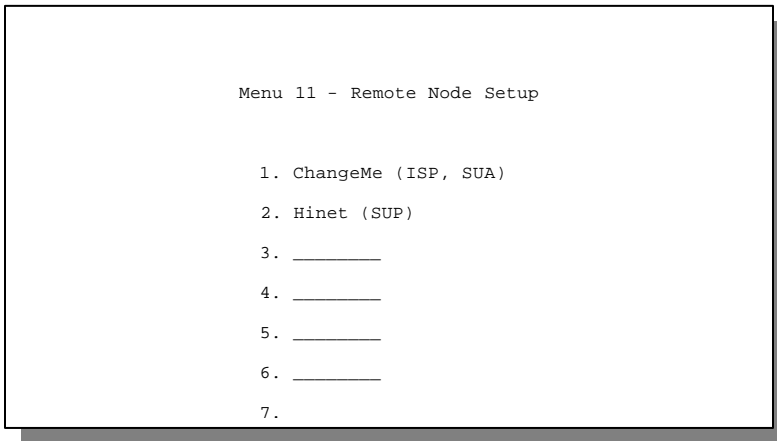


Figure 2 Remote Node Setup

IP Alias

Basics

The P480 supports three logical LAN interface via its single physical Ethernet interface. The Prestige is the gateway for all the LAN networks. You can also route packets from one network to another. The IP alias feature allows your Prestige to have extra IP addresses that may be in completely different subnets than the first IP address. The ability to partition physical network into logical network over the same Ethernet interface is referred to as IP Alias functionality.

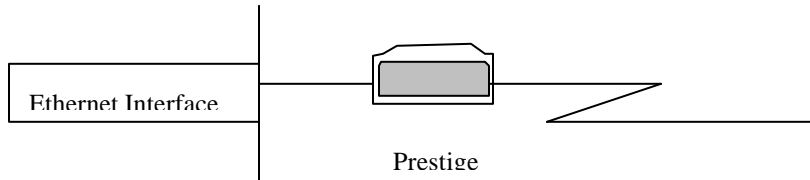


Figure 3 Physical Network

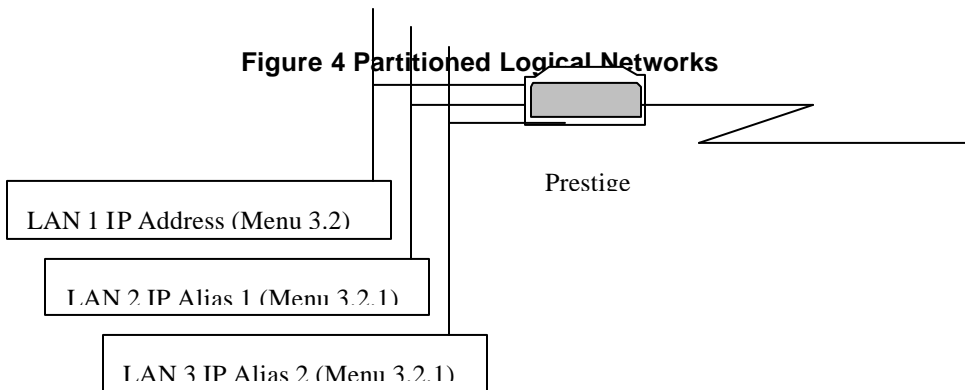


Figure 4 Partitioned Logical Networks

For example, in a school you can partition the single physical network into administration network, teachers network and students network as shown next.

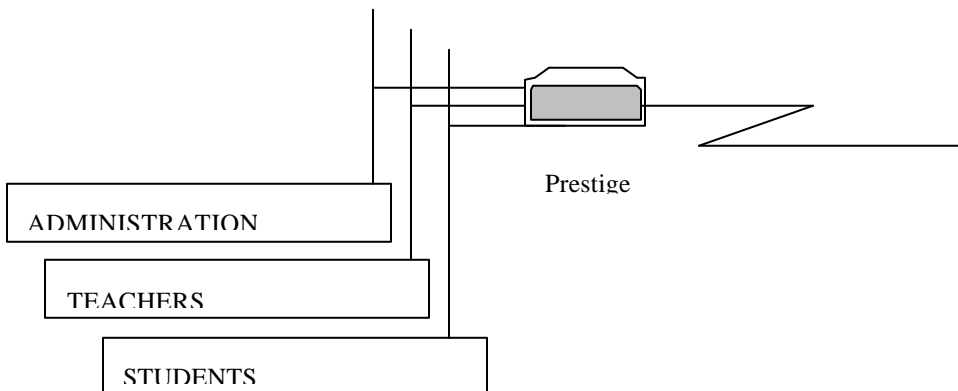


Figure 5 IP Alias Example

IP Alias Setup

You must use **Menu 3.2** to configure the first network and move the cursor to **Edit IP Alias** field and toggle

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup:
  DHCP= None
  Client IP Pool Starting Address= N/A
  Size of Client IP Pool= N/A
  Primary DNS Server= N/A
  Secondary DNS Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
  Version= RIP-2B
  Multicast = IGMP-v2
  IP Policies=
  Edit IP Alias= Yes

Enter here to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

the space bar to choose **Yes** and press [Enter] to configure the second and third network.

Figure 6 Menu 3.2 - TCP/IP and DHCP Ethernet Setup

Pressing [Enter] opens **Menu 3.2.1 - IP Alias Setup**, as shown next.

```
Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A
IP Alias 2= No
IP Address= N/A
```

Figure 7 Menu 3.2.1 - IP Alias Setup

Follow the instructions in the following table to configure IP Alias parameters.

Table 1 IP Alias Setup Menu Fields

Field	Description	Example
IP Alias	Choose Yes to configure the LAN network for the Prestige.	Yes
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.2.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press the space bar to select the RIP direction from Both/In Only/Out Only .	Both
Version	Press the space bar to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-1
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	

Protocol Filters	between this node and the Prestige.	
When you have completed this menu, press [Enter] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [Esc] at any time to cancel.		

IPX Configuration

This chapter shows you how to configure the IPX parameters of the Prestige.

IPX Network Environment

Novell bundles the protocol stack, the server software and routing functionality in their NetWare server products. So a NetWare server is not only a file or print server, it is also a router.

Network and Node Number

Every IPX machine has a network number and a node number, together they form the complete address of the machine. The IPX network number is a 32-bit quantity and is usually expressed in 8 hexadecimal digits, e.g., 0893A8CF. The host number is a 48-bit quantity and usually is taken from the MAC (Media Access Control) address of the Ethernet hardware, so you don't have to explicitly configure the node number.

An IPX client obtains its network number from a server that has the network numbers statically configured. If there are multiple servers on a network, only one server need to have the network numbers configured, and all other stations (clients and servers) can obtain the network numbers from it. The server with configured network numbers is called a seed router.

If you have a NetWare server on the same LAN as the Prestige, we recommend that you set up a NetWare server as a seed router. Even though the Prestige is capable of functioning as a seed router, a NetWare server offers a much more extensive facility for network management.

Frame Types

IPX can run on top of four different frame types on the Ethernet. These frame types are 802.2, 802.3, Ethernet II (DIX), and SNAP (Sub-Network Access Protocol). Each frame type is a separate logical network, even though they exist on one physical cable (see the following diagram).

Although there are four frame types available on the Ethernet, you should configure as few frame types as possible on your NetWare server and use automatic frame detection on the clients to simplify management and to reduce network overhead.

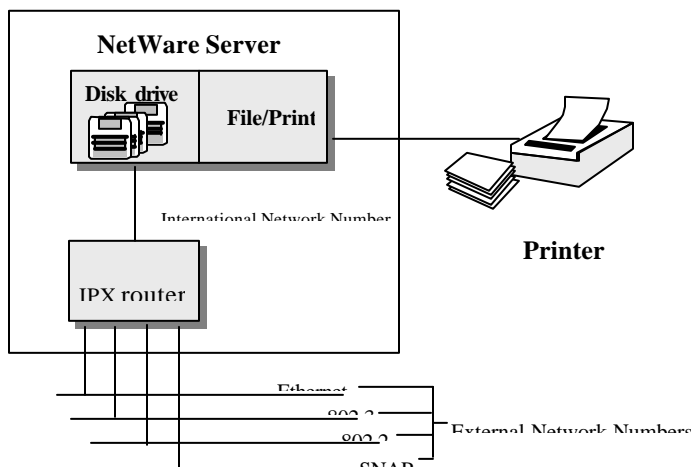


Figure 8 NetWare Server

External Network Number

Each of the four logical networks (based on frame type) has its own external network number.

Internal Network Number

In addition to the external network numbers, each NetWare server has its own internal network number that is a virtual network to which the server is attached. It is important to remember that every network number must be unique for that entire network, either internal or external.

Prestige in an IPX Environment

There are two scenarios in which your Prestige is deployed, depending on whether there is a NetWare server on the LAN or not, as depicted in the following diagram.

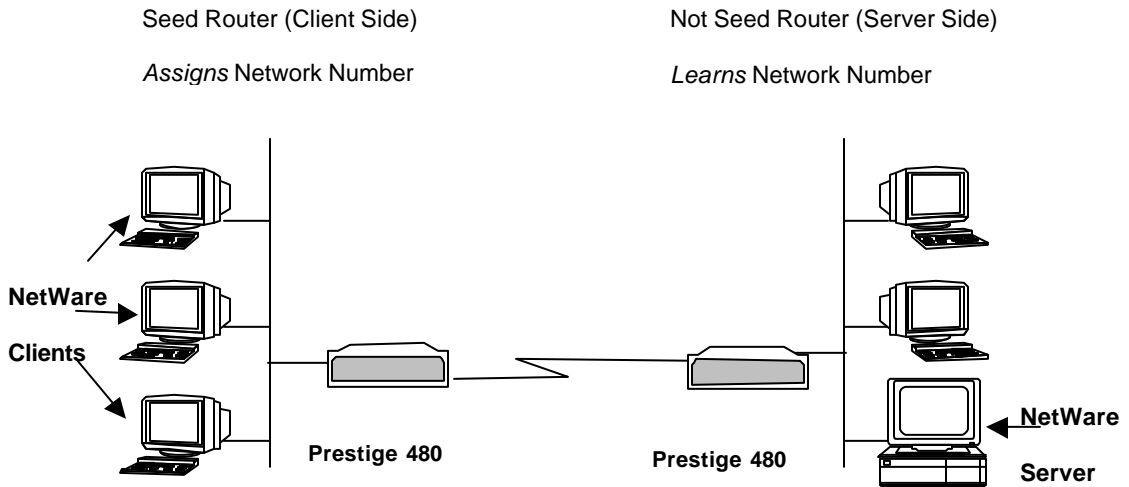


Figure 9 Prestige in an IPX Environment

Prestige on LAN with Server

If your Prestige is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your Prestige will learn the network number from the seed router and add the routes to its routing table.

Prestige on LAN without Server

Each IPX network must have a seed router. If you only have NetWare clients on your network, then you must configure the Prestige as a seed router and set up unique network numbers for each frame type enabled using the Ethernet Setup Menu.

IPX Spoofing

Your Prestige comes with several pre-defined call filters designed to prevent certain IPX packets from triggering a call to a remote node.

The built-in call filters are defined as follows:

- Block periodical RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) response messages.
- Block NetWare serialization packets.
- Allow SAP and RIP inquiry packets.

IPX Ethernet Setup

From Menu 3 - Ethernet Setup, select option **Novell IPX Setup** to go to **Menu 3.3 - Novell IPX Ethernet Setup** as shown in the next figure.

```
Menu 3.3 - Novell IPX Ethernet Setup

Seed Router= No

Frame Type 802.2= Yes
  IPX Network #= N/A

Frame Type 802.3= No
  IPX Network #= N/A

Frame Type Ethernet II= No
  IPX Network #= N/A

Frame Type SNAP= No
  IPX Network #= N/A

Enter here to CONFIRM or ESC to CANCEL:
Press Space Bar to Toggle.
```

Figure 10 Menu 3.3 - Novell IPX Ethernet Setup

The following table describes the Novell IPX Ethernet Setup Menu.

Table 2 Novell IPX Ethernet Setup Fields

Field	Description	Options
Seed Router	Determine if your Prestige is to act as a seed router.	Yes/No
Frame Type	Enable/Disable the individual frame type. Remember to enable only the ones that are actually used on your network.	802.2 802.3 Ethernet II SNAP
IPX Network #	If your Prestige is a seed router, enter a unique network number for each frame type enabled.	
Press [Enter] at the message [Press ENTER to Confirm ...] to save your configuration, or press [Esc] at any time to cancel.		

LAN-to-LAN Application with Novell IPX

A typical LAN-to-LAN application is to use your Prestige to call from a branch office to the corporate headquarters to enable the stations in the branch office to access the NetWare servers at the headquarters, as depicted in the next figure.

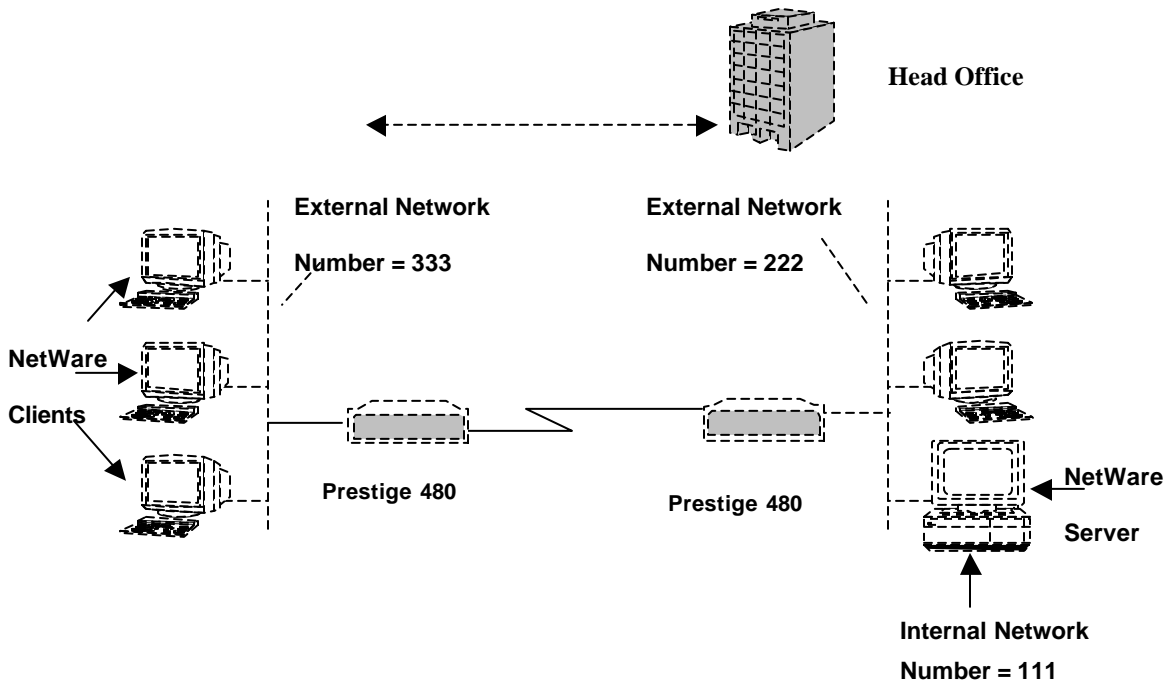


Figure 11 LAN-to-LAN Application with Novell IPX

IPX Remote Node Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in **Menu 11.1 - Remote Node Profile**. For the IPX-specific parameters in Menu 11.3 - Remote Node Network Layer Options follow the instructions below. If you want the Prestige to receive incoming calls, you must also configure the default dial-in parameters in Menu 13.

To edit Menu **11.3 - Remote Node Network Layer Options** shown next, follow these steps:

- Step 1.** In Menu 11.1, make sure **IPX** is among the protocols in the Route field. (The Route field should display Route = IPX or Route = IP + IPX.)
- Step 2.** Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space bar to select **Yes** and press [Enter] to open **Menu 11.3 - Network Layer Options**.

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:
Rem IP Addr:
Rem Subnet Mask= N/A
My WAN Addr= N/A
Single User Account= N/A
  Server IP Addr= N/A
Metric= N/A
Private= N/A
RIP Direction= N/A
  Version= N/A

IPX Options:
Dial-On-Query= No
Rem LAN Net #= 00000000
My WAN Net #= 00000000
Hop Count= 1
Tick Count= 2
W/D Spoofing(min)= 3
SAP/RIP Timeout(min)= 3

Bridge Options:
Dial-On-Broadcast= N/A
Ethernet Addr Timeout(min)= N/A

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 12 Menu 11.3 - Remote Node Novell IPX Options

The table below describes the IPX-specific parameters of the remote node setup.

Table 3 Remote Node Novell IPX Options

Field	Description	Option
Dial-On-Query	This field is necessary for your Prestige on the client side. When set to Yes , any Get Service SAP or RIP broadcasts will trigger your Prestige to make a call to that remote node.	Yes/No
Rem LAN Net #	In this field, enter the internal network number of the NetWare server on the remote LAN.	
My WAN Net #	In this field, enter the network number of the ISDN link. If you leave this field as 00000000 , your Prestige will determine automatically the network number through negotiation with the PPP peer.	00000000 (default)
Hop Count	This field indicates the number of intermediate networks that must be passed through to reach the remote node.	1 (default)
Tick Count	This field indicates the time-ticks required to reach the remote node.	2 (default)
W/D Spoofing (min)	This field is for the Prestige on the server side. Your Prestige can spoof a response to a server's WatchDog request after the connection is dropped. In this field, type in the time (number of minutes) that you want your Prestige to spoof the WatchDog response.	
SAP/RIP Timeout (min)	This field indicates the amount of time that you want your Prestige to maintain the SAP and RIP entries learned from this remote node in its internal tables after the connection has been dropped. If this information is retained, then your Prestige will not have to get the SAP information when the line is brought back up. Enter the time (number of minutes) in this field.	
Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm] to save your configuration, press [Esc] to cancel.		

IPX Static Route Setup

Similar to IP, IPX static routes tell the Prestige how to reach servers beyond a remote node before a connection to that remote node is established.

From Menu 12, select two, then select one of the IPX Static Routes to open **Menu 12.2.1 - Edit IPX Static Route**, as shown next.

```
Menu 12.2.1 - Edit IPX Static Route

Route #= ?
Server Name= ?
Active= Yes
Network #= ?
Node #= 000000000001
Socket #= 0451
Type #= 0004
Hop Count= 2
Tick Count= 3
Gateway Node= 1

Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 13 Menu 12.2 - Edit IPX Static Route

The following table contains the instructions on how to configure the Edit IP Static Route Menu.

Table 4 Edit IPX Static Route Menu Fields

Field	Description
Server Name	In this field, enter the name of the server. This must be the <i>exact</i> name configured in the NetWare server.
Network #	This field contains the internal network number of the remote server that you wish to access. [00000000] or [FFFFFFFF] are reserved.
Node #	This field contains the address of the node on which the server resides. If you are using a Novell IPX implementation, this value is [000000000001].
Socket #	This field contains the socket number on which the server will receive service requests. The default for this field is hex [0451].
Type #	This field identifies the type of service the server provides. The default for this field is hex [0004].
Gateway Node	In this field, enter the number of the remote node that is the gateway for this static route.
Hop Count and Tick Count	These two fields have the same meaning as those in the Ethernet setup.
Once you have completed filling in the menu, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel to cancel.	

Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige to transport packets of network layer protocols that the Prestige does not route, e.g., SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol and it also demands more CPU cycles and memory.

For efficiency reason, do *not* turn on bridging unless you need to support protocols other than IP and IPX on your network. For IP and IPX, enable the respective routing if you need it; do not bridge what the Prestige can route.

Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN; however, your Prestige applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the **Handle IPX** field.

From Menu 3 - Ethernet Setup, enter option **Bridge Setup** and **Menu 3.4 - Bridge Ethernet Setup** displays as shown next.

```
Menu 3.4 - Bridge Ethernet Setup

Handle IPX= Client

Press ENTER to CONFIRM or ESC to CANCEL:
Press Space Bar to Toggle.
```

Figure 14 Menu 3.5 - Bridge Ethernet Setup

The following table describes how to configure the **Handle IPX** field in Menu 3.5.

Table 5 Bridge Ethernet Setup Menu - Handle IPX Field Configuration

Handle IPX Field (Menu 3.5)	Description
None	When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX.
Client	When there are only client workstations on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls.
Server	When there are only IPX servers on the LAN. No RIP or SAP packets will trigger calls. In addition, during the time when the line is down, your Prestige will reply to watchdog messages from the servers on behalf of remote clients. The period of time that your Prestige will do this is linked to the Ethernet Address Timeout parameter in each remote node (see Remote Node Configuration). When a remote Ethernet address is aged out, there is no need to maintain its connection to the IPX server.

If there are both clients and servers on the LAN, and the local clients will access the remote servers, set this field to **Server** but turn on the **Dial-On-Broadcast** parameter in Menu 11.3 to allow the client queries to trigger calls.

Remote Node Bridging Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in **Menu 11.1 - Remote Node Profile**. For bridging-specific parameters, you need to configure **Menu 11.3 - Remote Node Network Layer Options**.

To setup **Menu 11.3 - Remote Node Network Layer Options**, follow these steps:

- Step 1.** In Menu 11.1, make sure the **Bridge** field is set to **Yes**.
- Step 2.** Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space bar to select **Yes** and press [Enter] to open **Menu 11.3 - Network Layer Options**.

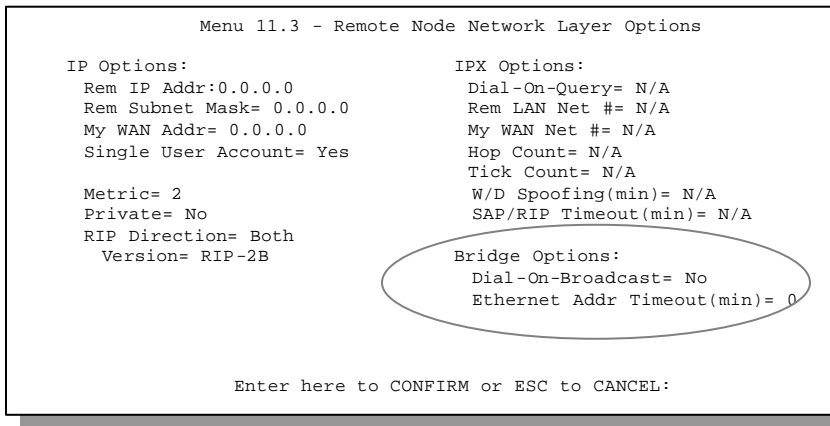


Figure 15 Menu 11.3 - Remote Node Bridging Options

The following table describes the bridging-specific parameters in the Remote Node Profile and Network Layers menus.

Table 6 Remote Node Network Layers Menu Bridge Options

Field	Description
Bridge	Make sure this field is set to Yes .
Edit IP/IPX/Bridge	Press the space bar to change it to Yes and press [Enter] to go to the Network Layer Options Menu.
Dial-On-Broadcast	This field is necessary for your Prestige on the caller side LAN. When set to Yes , any broadcasts coming from the LAN will trigger your Prestige to make a call to this remote node. If it is set to No , your Prestige will not make the outgoing call.
Ethernet Addr Timeout (min)	In this field, enter the time (number of minutes) that you wish your Prestige to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line is brought back up.

Once you have completed filling in the Network Layer Options Menu, press [Enter] to return to Menu 11.1. Then press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel.

Bridge Static Route Setup

```
Menu 12.3 - Bridge Static Route Setup
1. _____
2. _____
3. _____
4. _____

Enter selection number:
```

Similar to network layer static routes, a bridging static route tells the Prestige about the route to a node before a connection is established. You configure bridge static routes in Menu 12.3.1, by pressing 3 in menu 12 and then selecting one of the bridge static routes as shown next.

Figure 16 Menu 12.3 - Bridge Static Route Setup

```
Menu 12.3.1 - Edit Bridge Static Route

Route #: 1
Route Name= ?
Active= No
Ether Address= ?
IP Subnet Mask=
Gateway IP = 1

Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 17 Menu 12.3.1 - Edit Static Route

The following table describes the Bridge Static Route Menu.

Table 7 Bridge Static Route Menu Fields

Field	Description
Route Name	Enter a name for the bridge static route for identification purposes.
Active	Activate/deactivate the static route.
Ether Address	Enter the MAC address of the destination machine that you wish to bridge the packets to.
IP Address	If available, enter the IP address of the destination machine that you wish to bridge the packets to.
Gateway Node	Enter the number of the remote node that is the gateway of this static route. When a packet's destination Ethernet (MAC) address matches the value entered above, it will trigger a call to this remote node.
Once you have completed filling in this menu, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel.	

NetCAPI Support

Basics

NetCAPI is ZyXEL's implementation of CAPI (Common ISDN Application Program Interface) capabilities over a network. It runs over DCP (Device Control Protocol) developed by RVS-COM.

NetCAPI can be used for applications such as Eurofile transfer, file transfer, G3/G4 Fax, Autoanswer host mode, telephony, etc. on Windows 95/98/NT platforms.

CAPI

CAPI is an interface standard that allows applications to access ISDN services. Several applications can share one or more ISDN lines. When an application wants to communicate with an ISDN terminal it sends a series of standard commands to the terminal. The CAPI standard defines the commands and allows you to use a well-defined mechanism for communications using ISDN lines.

CAPI also simplifies the development of ISDN applications through many default values that do not need to be programmed. It provides a unified interface for applications to access the different ISDN services such as data, voice, fax, telephony, etc.

ISDN-DCP

ISDN-DCP allows a workstation on the LAN to use services such as transmitting and receiving faxes as well as placing and receiving phone calls.

Using ISDN-DCP, the Prestige acts as a DCP server. By default, the Prestige listens for DCP messages on TCP port number 2578 (the Internet-assigned number for RVS-COM DCP). When the Prestige receives a DCP message from a DCP client i.e., a workstation, the Prestige processes the message and acts on it. Your Prestige supports all the DCP messages specified in the ISDN-DCP specification.

RVS-COM

RVS-COM includes an ISDN CAPI driver with its communication program. RVS-CE (Core Engine) is an ISDN-CAPI 2.0 driver for Windows 95/98/NT that can be used by different ISDN communication programs (such as AVM Fritz or RVS-COM) to access the ISDN on the Prestige.

NetCAPI can carry out CAPI applications only if the CAPI driver is installed on your workstation. In addition to the CAPI driver, you will need a communication software program such as RVS-COM Lite, Fritz etc., for users to access CAPI.

The ISDN router is a shared device and can be used by several different client workstations at the same time: e.g. one workstation sending a fax, another workstation doing a file transfer. RVS-COM has to be installed on each client workstation in order to share the ISDN lines

Configuring the P480 as a NetCAPI Server

This section describes how to configure your Prestige to be a NetCAPI server using the SMT (System Management Terminal).

[**Note** : For configuring your Prestige with the PNC, use PNC ISDN Series version 2.20 and above.]

By default, NetCAPI is enabled on your Prestige. When NetCAPI is enabled, the Prestige listens for incoming DCP messages from the workstations. By default, the Prestige listens for DCP messages on TCP port 2578.

The following figure illustrates the configuration used in this example.

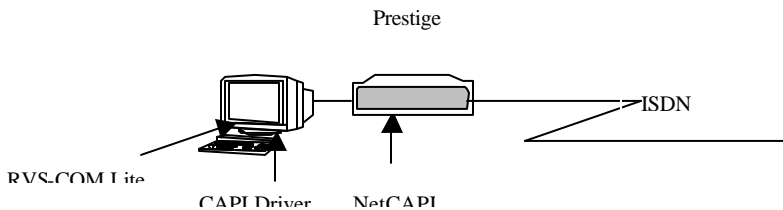


Figure 18 Configuration Example

Before entering any configurations, you must install the CAPI driver and communication program such as RVS-COM Lite on your workstation.

Installing the CAPI driver and Communication Software

[**Note:** Please uninstall previous versions of "RVS -CAPI" and "RVS-COM lite" before you install the new versions. You may use the Windows "START | Settings | Control Panel | Add/Remove Programs" to uninstall RVS-CAPI and RVS-COM.]

To install the CAPI driver and the communication software, enter one of the license keys of your RVS-COM Lite CD-ROM and follow the instructions on the configuration wizard. When you install RVS-Lite, RVS-COM AUTOMATICALLY installs CAPI driver before installing RVS-Lite.

Note: If you did not install RVS-Lite and want to use other programs such as AVM Fritz to access the ISDN router, you must first install the CAPI driver - RVS-CE using the English version installation wizard (in \DISKs\CEPE\DISK1\) and start the SETUP.EXE.

Configuring NetCAPI

Step 1. Go to **Menu 2 - ISDN Setup.**

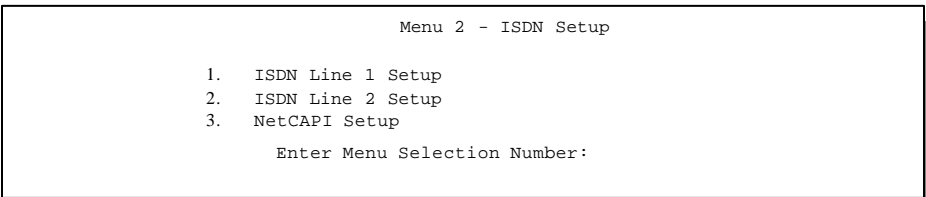


Figure 19 Menu 2 - ISDN Setup

Step 2. Enter 3 and press [Enter] to go to **Menu 2.3 - NetCAPI Setup.**

```
Menu 2.3 - NetAPI Setup

Active= Yes

Max Number of Registered Users= 1
Incoming Data Call Number Matching= MSN

Access List:
  Start IP      End IP      Operation
  192.168.1.132 192.168.1.145 Both
  192.168.14.1  192.168.14.32 Incoming
```

Figure 20 Menu 2.3 - NetAPI Setup

Step 3. Set the fields in the **NetCAPi Setup** menu according to the following description.

Table 8 NetCAPi Setup Fields

Field	Description
Active	This field allows you to enable or disable NetCAPi. Press the [Spacebar] to toggle between Yes and No
Max Number of Registered Users	When you want to use NetCAPi to place outgoing calls or to listen to incoming calls, you must start RVSCOM on your workstation, and RVSCOM will register itself to the Prestige. This option is the maximum number of clients that the Prestige supports at the same time. The default value is 4 .
Incoming Data Call Matching	<p>This field determines how incoming calls are routed. Press the [Spacebar] to select NetCAPi if you want to direct all incoming data calls to NetCAPi.</p> <p>Select MSN if you want to direct all incoming call to the Prestige only when the incoming phone number matches the ISDN DATA number in Menu 2. If the incoming phone number does not match the ISDN DATA number, then the call will be routed to NetCAPi.</p> <p>Select Called Party Subaddress if you want to direct all incoming calls to the Prestige only when the incoming call matches the subaddress of ISDN DATA in Menu 2. If the incoming call does not match the subaddress of ISDN DATA, then the call will be routed to NetCAPi.</p>
Access List	<p>This list specifies users that can use NetCAPi. This access list controls if a client is allowed to use NetCAPi. The request is rejected when</p> <ol style="list-style-type: none"> 1. The IP address of the workstation is not between Start IP and End IP or 2. The request from the workstation is not permitted as specified in the Operation field.
Start IP	Refers to the first IP address of a group of NetCAPi clients. Each group contains contiguous IP addresses.
End IP	Refers to the last IP address in a NetCAPi client group.
Operation	<p>Press the [Spacebar] to select Incoming if you wish to grant incoming calls permission. Select Outgoing if you wish to grant outgoing calls permission. Select Both if you wish to grant both incoming calls and outgoing calls permissions. Select None if you wish to deny all calls.</p>

RADIUS Accounting

In addition to the local error/trace log and UNIX syslog, the Prestige also supports RADIUS accounting. This facility logs information about dial-in connections. The RADIUS accounting server may be located on the same host as the RADIUS authentication server, or on a separate host. RADIUS accounting can be configured in **Menu 24.3.3 – System Maintenance – Accounting Server** as shown next.

```
Menu 24.3.3 - System Maintenance - Accounting Server

Accounting Server:
Active= No
Type: RADIUS
Server Address= ?
Port #= 1646
Key= ?

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 21 Menu 24.3.3 – System Maintenance – Accounting Server

The fields in **Menu 24.3.3** are listed in the following table.

Table 9 Menu 24.3.3 System Maintenance – Accounting Server Fields

Field	Description
Active	Determines whether the accounting facility is on or off.
Type	Determines the type of the accounting server. At present only RADIUS is supported.
Server Address	The IP address of the accounting server.
Port #	The IP port number used by the accounting server. The default is port 1646.
Key	The “password” used to authenticate your Prestige to the RADIUS service. Please note that this is between the Prestige and the server; it has nothing to do with the dial-in users.

Once the accounting server is enabled and the RADIUS external server authenticates users, the Prestige sends messages to the external server. Some examples are shown next.

```

Fri Aug 13 11:22:03 1999

    Acct-Status-Type = Start

    Acct-Session-Id = "23850000000002"

    User-Name = "ras"

    NAS-Port = 131072

    NAS-Port-DNIS = "5553100"

    Caller-Id = "5552100"

```

Figure 22 Examples of RADIUS Accounting Message

The following table describes the accounting attributes mentioned in the above example.

Note: Accounting attributes may vary depending on the external server.

Table 10 Accounting Attributes

Field	Description
Acct-Status-Type	Account Status Type has four values: Accounting On, Accounting Off, Start and Stop. An Accounting On record is created when the Prestige starts the RADIUS Accounting service. An Accounting Off record is created when the Prestige ends the service. A Start record is created when a user session begins. A Stop record is recorded when the session ends.
Acct-Session-Id	Account Session Id is a unique number assigned to each Start and Stop record to make it easy to match the Start and Stop records in a detail file, and to eliminate duplicate records. Note that in the above example this value matches in the Start and Stop record, indicating that these records correspond to the same session.
User-Name	Specifies the user name.
NAS-Port	Refers to the Network Access Server (NAS) port used in the connection.
NAS-Port-DNIS	Refers to the called party's directory number.

Caller Id	Refers to the dial-in-user's Caller ID.
-----------	---

Backup and Restore Configuration Using FTP

Back up using FTP

To transfer the firmware and the configuration file, follow the procedure below:

- Step 1.** Launch the FTP client on your workstation.
- Step 2.** Type `open` and the IP address of your Prestige. Then type `root` and your SMT password as requested.
- Step 3.** Locate the “`rom-spt`” file.
- Step 4.** Type `get rom-spt` to backup the current Prestige configuration to your workstation.

For details on FTP commands, please consult the documentation of your FTP client program.

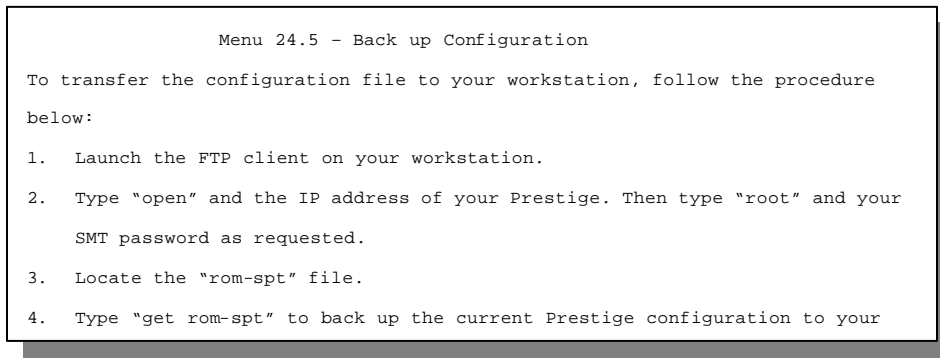


Figure 23 Backup Configuration using FTP

Restore using FTP

Even though FTP should work over WAN as well, it is not recommended.

To transfer your current workstation configuration to your Prestige, follow the procedure below:

- Step 1.** Launch the FTP client on your workstation.
- Step 2.** Type `open` and the IP address of your Prestige. Then type `root` and password as requested.
- Step 3.** Type `put backupfilename rom-spt` where “*backupfilename*” is the name of your backup configuration file on your workstation and “*rom-spt*” is the remote file name on the Prestige. This restores the configuration to your Prestige.
- Step 4.** The system reboots automatically after the file transfer process is complete.

For details on FTP commands, please consult the documentation of your FTP client program.

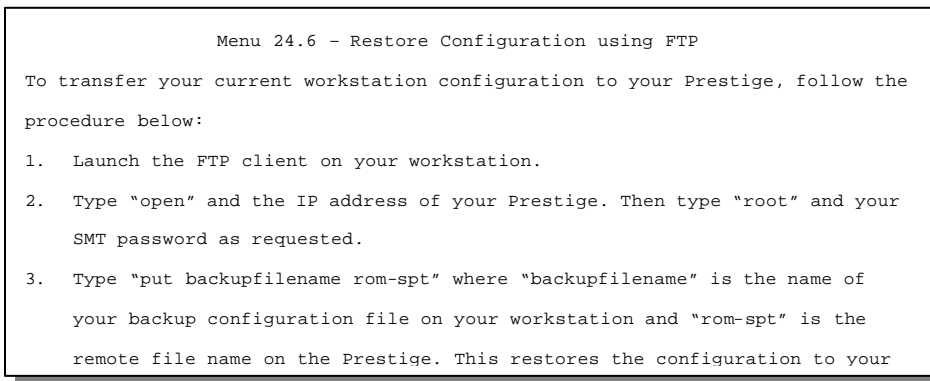


Figure 24 Restore Configuration using FTP

Firmware and Configuration Files Upload via FTP Clients

In addition to uploading the firmware and configuration via the console port and TFTP client, you can also upload the P480 firmware and configuration files using FTP.

To use this feature, your workstation must have an FTP client. To transfer the firmware and the configuration file, follow the examples below:

Using FTP command in terminal

- Step 1.** Use FTP client from your workstation to the Prestige 480 and log in by entering the IP address of the Prestige.
- Step 2.** Press [ENTER] key to ignore user name.
- Step 3.** Enter the administrator password. The default is 1234
- Step 4.** Enter the command “bin” to set binary transfer type
- Step 5.** Use the command “put” to transfer files between the Prestige and the workstation. The file name

```
Connected to 480.x.x.x
220 P480 FTP version 1.0 ready at Thu Jan  8 18:00:02 1970
User (480.x.x.x:(none)): <Enter>
331 Enter PASS command
Password:
230 Logged in
ftp> bin
ftp> ha
```

for the firmware is "ras" and for the configuration file "rom-0" (rom-zero, not capital o).

Figure 25 FTP Example

The system reboots after a successful upload.

Using FTP client software

- Step 1.** Rename the local firmware and configuration files to '**ras**' and '**rom-0**', because we can not specify the remote file name in the FTP client software.
- Step 2.** Use FTP client from your workstation to the Prestige 480 and log in by entering the IP address of the Prestige.
- Step 3.** Set the transfer type to '**Auto-Detect**' or '**Binary**'.

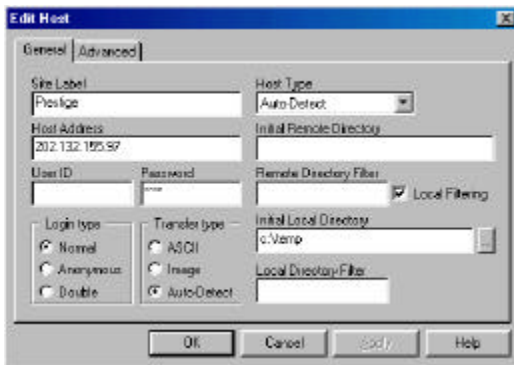


Figure 26 Edit Host

- Step 4.** Press '**OK**' to ignore the 'Username' prompt.



Figure 27 Username Prompt

- Step 5.** To upload the firmware file, transfer the local '**ras**' file to overwrite the remote '**ras**' file.
To upload the configuration file, transfer the local '**rom-0**' to overwrite the remote '**rom-0**' file.

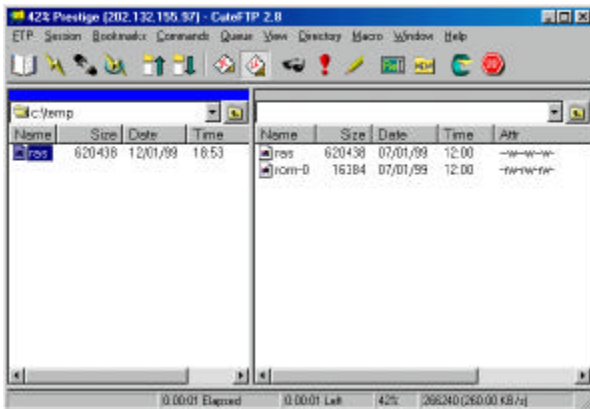


Figure 28 Files Transfer

The system reboots after a successful upload.

IP Policy Routing

Introduction

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

Routing Policy

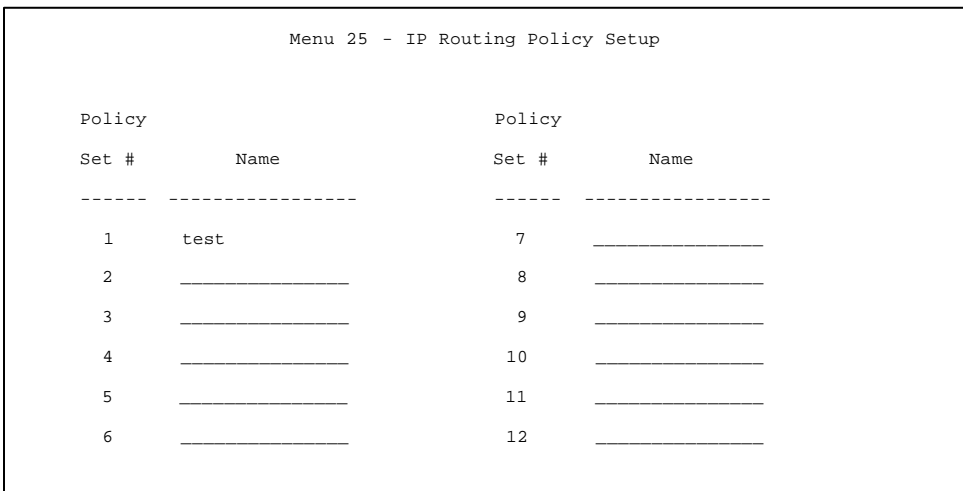
A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

IP Routing Policy Setup

Menu 25 shows all the policies defined



The screenshot shows a terminal window titled "Menu 25 - IP Routing Policy Setup". It displays a table with two columns of "Policy" information. The left column lists Set # 1 through 6, with the name "test" for Set 1 and blank lines for Sets 2-6. The right column lists Set # 7 through 12, all with blank lines. The table is separated by dashed lines.

Policy		Policy	
Set #	Name	Set #	Name
1	test	7	
2		8	
3		9	
4		10	
5		11	
6		12	

Figure 29 Menu 25 - IP Routing Policy Setup

To setup a routing policy, follow the procedures below:

Step 1. Enter 25 in the Main Menu to open **Menu 25 – IP Routing Policy Setup**.

Step 2. Enter the index of the policy set you wish to configure to open **Menu 25.1 - IP Routing Policy Summary**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the

incoming packet, and the latter is the action. Between these two parts, separator '|' means the action is taken on criteria matched and separator '=' means the action is taken on criteria not matched.

```
Menu 25.1 - IP Routing Policy Summary

# A          Criteria/Action
- - - - -
1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
    SP=20-25,DP=20-25,P=6,T=NM,PR=0      |GW=192.168.1.1,T=MT,PR=0
2 N _____
    _____
3 N _____
    _____
```

Figure 30 Menu 25 - IP Routing Policy Summary

Table 11 IP Routing Policy Summary

Abbreviation	Meaning
Criteria	
SA	Source IP address
SP	Source port
DA	Destination IP address
DP	Destination port
P	IP layer 4 protocol number(TCP=6,UDP=17...)
T	Type Of Service of Incoming packet
PR	Precedence of incoming packet
Action	
GW	Gateway IP address
T	Outgoing Type of Service
P	Outgoing Precedence
Type Of Service	
NM	Normal
mD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

Enter a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= test
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Normal      Packet length= 40
  Precedence      = 0          Len Comp=
  Source:
    addr start= 1.1.1.1      end= 1.1.1.1
    port start= 20          end= 20
  Destination:
    addr start= 2.2.2.2      end= 2.2.2.2
    port start= 20          end= 20
  Action= Matched
  Gateway Type    = Gateway node   Gateway addr = 1.2.3.4
  Type of Service= No Change        Gateway node = 2
  Precedence     = No Change        Log= No

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

Figure 31 Menu 25.1.1 - IP Routing Policy

Table 12 IP Routing Policy

Field	Description
Policy Set Name	This is the name of the policy set assigned in Menu 25 - IP Routing Policy Setup.
Active	Press the spacebar to select Yes to activate the policy.
Criteria	
IP Protocol	IP layer 4 protocol, e.g., UDP, TCP, ICMP, etc.
Type of Service	Prioritize incoming network traffic by choosing from Don't Care/ Normal / Min Delay / Max Thruput / Max Reliability .
Packet Length	Enter the length of incoming packets (in bytes). The operators in the [Len Comp] (next) apply to packets of this length.
Len Comp	Press the spacebar to choose from Equal / Not Equal / Less / Greater / Less or Equal / Greater or Equal .
Precedence	Precedence value of the incoming packet. Values range from 0 to 7 or Don't Care .
Source:	
addr start= / end=	Source IP address range from start to end.

port start= / end=	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start= / end=	Destination IP address range from start to end.
port start= / end=	Destination port number range from start to end; applicable only for TCP/UDP.
Action=	Specifies whether action should be taken on criteria Matched or Not Matched .
Gateway type	Allows you to choose the outgoing gateway type. The gateway can be on the same subnet as the Prestige if it's on the LAN, otherwise, the gateway can be the IP address of a remote node. You can choose Gateway addr if you want to assign the gateway IP address by yourself. Or you can specify the remote node as your gateway by choosing Gateway node .
Gateway addr	Enter the IP address of your gateway.
Gateway node	This can be set as 0 to 12. 0 means no change. 1 means remote node 1 in Menu 11 and so on.
Type of Service	Set the new TOS value of the outgoing packet. Choose from Prioritize incoming network traffic by choosing from No Change / Normal / Min Delay / Max Thruput / Max Reliability .
Precedence	Set the new precedence value of the outgoing packet. Values range from 0 to 7 or No Change .
Log	Press the spacebar to select Yes to make an entry in the system log when a policy is executed.

Applying an IP Policy

This section shows you where to apply the IP Policies after you design them.

Ethernet IP Policies

From **Menu 3 - Ethernet Setup**, enter 2 to go to **Menu 3.2 -TCP/IP Ethernet Setup**.

You can choose up to four IP Policy sets (from twelve) by entering their numbers separated by commas, e.g., 2, 4, 7, 9.

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A

TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP- 1
  Multicast = IGMP-v2
  IP Policies=
  Edit IP Alias= Yes

Enter here to CONFIRM or ESC to CANCEL:
Press Space Bar to Toggle.
```

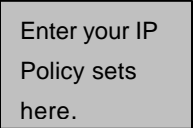


Figure 32 Menu 3.2 – TCP/IP Ethernet Setup