ZyXEL

Prestige 128IMH
Technical Assistance

ZyXEL Prestige P128IMH

2.21 Release Note

Date: January 18, 1999

Congratulations on your purchase of a ZyXEL Prestige 128IMH Remote Access Router. In a modem-sized box, the Prestige 128IMH offers inexpensive yet complete telecommunications and internetworking solutions for your home or branch office. The Prestige 128IMH is ideal for everything from surfing the Internet to receiving calls from Remote Dial-in Users to making LAN-to-LAN connections to Remote Nodes.

Distinguishing features of the Prestige 128IMH include Remote Dial-in User support, an Internet Single User Account (Network Address Translation), POTS line support (Plain Old Telephone Service; also called A/B Adapter in Europe), extensive Network Management, built-in 4-port Ethernet hub, and the latest security features.

Features

The Prestige 128IMH is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

ISDN Basic Rate Interface (BRI)

Using either a standard BRI S/T Interface or U Interface the Prestige supports a full range of switch types. The switch type depends on the Central Office switch your ISDN line is connected to. The two B-channels can be used independently for two destinations, or they can be bundled for a single connection with PPP/MP.

Built-in V.90 Client site Modem

The Prestige has a built-in V.90 client site modem. This enables it to communicate to remote routers or users at speeds up to 56 Kbps through the ISDN connection.

Multiple Networking Protocol Support

The Prestige is a multi-protocol router. It supports TCP/IP, Novell IPX, and Transparent Bridging.

Analog Phone Ports

The Prestige is equipped with two standard phone jacks to connect to telephones, FAX machines, or modems. This allows the ISDN line to be used for voice calls as well as data calls.

Caller Display Services on Analog PSTN lines

Prestige support to send out CLID information on both POST ports. To use Caller Display you need a special telephone or display unit which show, and then store, the numbers of incoming callers.

Supplementary Voice Features

The Prestige supports the following Supplementary Voice Features on both of its Analog (POTS) Phone Ports:

Call Waiting

Three Way Calling (conference)

Call Transfer

Call Forwarding

Reminder Ring

Remote Dial-in Users

The Prestige has a built-in V.90 client site modem. This allows users that have workstations with remote access capabilities to dial-in to the Prestige to access network resources not only through ISDN network but also PSTN network.

Built-in 4-Port Ethernet Hub

The Prestige 128IMH is equipped with a built-in 4-port Ethernet hub. The built-in hub eliminates the need to purchase a separate hub when building a one to four-port network. For a larger number of workstations, an additional hub may be connected using a crossover cable.

Dial-on-Demand

The Dial-on-Demand feature allows the Prestige to automatically place a call to a Remote Node whenever there is traffic coming from any workstation on the LAN to that remote site.

Bandwidth-on-Demand

The Prestige supports bandwidth up to 128Kbps over a single ISDN BRI line. It incorporates PPP/MP (Point-to-Point Protocol/Multilink Protocol) to bundle two B channels over a BRI line. In addition, the Prestige dynamically allocates bandwidth between the two B channels, increasing or decreasing speeds as needed to allow for greater efficiency in data transfer. It supports BAP (Bandwidth Allocation Protocol) and BACP (Bandwidth Allocation Control Protocol) to manage the number of links in multilink bundle.

Network Management

The Prestige supports two methods of system management: The SMT interface and the Prestige Web Configurator.

SMT Interface

The SMT interface is a menu driven network management interface which can be accessed via an RS-232 interface or a Telnet connection.

Prestige Web Configurator

The Prestige Web Configurator is a JAVA based utility designed to allow users to access the Prestige's management settings via a Worldwide Web browser.

Backup and Restore Configuration File via LAN or WAN

PCT (Prestige Configuration Transfer), the stand-alone Java-based utility, allows backup and restoration of the configuration file via LAN or WAN.

Upgrade P128IMH Firmware via LAN

PCT can upgrade the Prestige128IMH firmware over the local LAN.

DHCP Support (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows you to automatically assign IP address settings to workstations on your network.

Security

The Prestige supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).

RADIUS (Remote Authentication Dial In User Service)

The RADIUS feature allows you to use an external, central, Unix based server to support thousands of users.

Call Control

The Prestige provides budget management for outgoing calls and maintains a blacklist for unreachable phone numbers in order to save you the expense of unnecessary charges.

Data Compression

The Prestige incorporates Stac data compression and CCP (Compression Control Protocol).

Networking Compatibility

The Prestige is compatible with remote access products from other companies such as Ascend, Cisco, and 3Com. Furthermore, it supports Microsoft Windows 95 and Windows NT remote access capability.

Applications For Your Prestige

Some applications for the Prestige include:

Internet Access

The Prestige supports the TCP/IP protocol, which is the language used for the Internet. It is also compatible with access servers manufactured by major vendors such as Cisco and Ascend.

Internet Single User Account (SUA)

For a small office environment, the Prestige offers a Single User Internet Account from an ISP (Internet Service Provider). This allows for unlimited users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single user.

Single User Account address mapping can also be used for LAN to LAN connection.

Multiprotocol LAN-to-LAN Connection

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

Telecommuting Server

The Prestige allows Remote Dial-in 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 dial in using an ISDN terminal adapter (TA) to access the network resources without physically being in the office.

Nailed-up Connection

This new feature allows a dial-up line to emulate a leased line.

Features Details

How to make and answer a modem call by Prestige 128IMH Internal Modem

To make a modem call by Prestige P128IMH Internal Modem

At menu 4 and menu 11, select the Telco Option Transfer Type = Modem, the call to these ISP or remote nodes wil be made through internal modem.

```
                    Menu 4 - Internet Access Setup

                ISP's Name= ChangeMe
                Pri Phone #= 1234
                Sec Phone #=
                My Login= ChangeMe
                My Password= ********
                Single User Account= Yes
                  IP Addr= 0.0.0.0

                Telco Options:
                  Transfer Type= Modem

                Multilink= N/A
                Idle Timeout= 300

                Press ENTER to Confirm or ESC to Cancel:
```

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe             Route= IP
Active= Yes                         Bridge= No

Call Direction= Outgoing            Edit PPP Options= No
Incoming:                           Rem IP Addr= 0.0.0.0
  Rem Login= N/A                      Edit IP/IPX/Bridge= No
  Rem Password= N/A                 Telco Option:
  Rem CLID= N/A                       Allocated Budget(min)= 0
  Call Back= N/A                      Period(hr)= 0
Outgoing:                             Transfer Type= Modem
  My Login= ChangeMe                  Nailed-Up Connection= No
  My Password= ********             Session Options:
  Authen= CHAP/PAP                    Edit Filter Sets= No
  Pri Phone #= 1234                   Idle Timeout(sec)= 300
  Sec Phone #=

                Press ENTER to Confirm or ESC to Cancel:
```

Menu 11.1 - Remote Node Profile

To answer a modem call by Prestige P128IMH Internal Modem

At menu 2, select Enable to accept modem call. For DSS1 switch type, select MSN will help you match the modem call phone number at A/B adapter 2. If you do not apply MSN, you can select Don't Care option, and enable A/B Adapter 2 accept modem call. This setting can let you answer the modem call by A/B Adapter 2, however it also routes your voice call to internal modem. Since there is no way to distinguish the incoming call is modem or voice call. It will be a little inconvenient to you if you do not apply the MSN services

.

And when you use the internal modem for out call or answering a call, the A/B Adapter 2 can not be used for voice call. The same reason, when you use A/B Adapter 2 for voice call, you can not make a modem call or answer a modem call. That is, A/B Adapter 2 and internal modem share the same HW resource, so you can't use both two at the same time.

```
                          Menu 2 - ISDN Setup
        Switch Type: DSS-1(Taiwan)
        B Channel Usage= Switch/Switch

        ISDN Data     =   10000              Subaddress=
        A/B Adapter 1 =  10001              Subaddress=
        A/B Adapter 2 =  10002              Subaddress=
        A/B Adapter 2 Accepts Modem Call= Enable

        Dial Prefix to Access Outside Line=
        PABX Number (Include S/T Bus Number)=
        Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
          Analog Call Routing= N/A
          Global Analog Call= N/A

     Advance Setup = No
                   Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Menu 2 - ISDN Setup for DSS1 (European) by MSN

```
                          Menu 2 - ISDN Setup
        Switch Type: DSS-1(Taiwan)
        B Channel Usage= Switch/Switch

        ISDN Data     =                    Subaddress=
        A/B Adapter 1 =                    Subaddress=
        A/B Adapter 2 =                    Subaddress=
        A/B Adapter 2 Accepts Modem Call= Enable

        Dial Prefix to Access Outside Line=
        PABX Number (Include S/T Bus Number)=
        Incoming Phone Number Matching= Don't Care
          Analog Call Routing= N/A
          Global Analog Call= Accept

        Advance Setup = No
                   Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Menu 2 - ISDN Setup for DSS1 (European) by Don't Care

DHCP Server

By default, Prestige is now configured as a DHCP server. The range of IP address pool is from 192.168.1.33 to 192.168.1.64. The DNS Proxy feature is enabled. Please refer to the DNS Proxy sub-section for details.

Menu 3.2:

```
        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

                  TCP/IP Setup:
                    IP Address= 192.168.1.1
                    IP Subnet Mask= 255.255.255.0
                    RIP Direction= Both
                      Version= RIP-1
```

SUA and Dynamic IP Address

By default, both SUA and dynamic IP address are enabled. By utilizing the factory default configuration, it will be easy to most of new customers to start to browse the Internet in minutes.

Menu 4:

```
            Menu 4 - Internet Access Setup

                 ISP's Name= ChangeMe
                 Pri Phone #= 1234
                 Sec Phone #=
                 My Login= ChangeMe
                 My Password= ********
                 Single User Account= Yes
                   IP Addr= 0.0.0.0

                 Telco Options:
                   Transfer Type= 64K

                 Multilink= Off
                 Idle Timeout= 300
```

DNS Proxy

If enabled, DNS Proxy will allow the Prestige to act as the DNS server for the local network. The Prestige will get the IP address of the actual DNS server from the remote site via IPCP negotiation. Note this feature only works if the remote site supports RFC 1877.

Configuring the DNS Proxy

DNS Proxy is enabled only if the selection of the *DHCP* field under *DHCP Setup* in Menu 3.2 is *Server* and the *Primary DNS Server* field in Menu 3.2 is set to *0.0.0.0*. (This is factory default). If DNS Proxy is enabled , the Prestige will assign its IP address as the Primary DNS in the responses to DHCP requests on the local network. SMT enforces the consistency between the *Primary DNS server* and *Secondary DNS server* fields in Menu 3.2 by skipping *Secondary DNS Server* field if the IP address of the *Primary DNS Server* field is 0.0.0.0.

If the selection of the ***DHCP*** field under ***DHCP Setup*** in Menu 3.2 is ***None***, both of DHCP Server and DNS Proxy functions are disabled. Prestige will assign the values entered in ***Primary DNS server*** and ***Secondary DNS server*** fields in Menu 3.2 to the responses to the DHCP requests on the local network if DHCP Server function is enabled.

DNS Proxy Functional Flows

If DNS Proxy is enabled, Prestige will perform the following functions after receiving a DNS request from local network:

1. If there is no ISP configuration (default remote node), this DNS request packet will be discarded. Otherwise, continue.
2. Save this DNS request in an internal table.

3. If the connection to ISP is not up, Prestige will attempt to bring up the connection and negotiate with the remote site for the DNS server. Otherwise, continue.
4. If there is no DNS server negotiated on the connection to ISP, Prestige will discard this DNS request from the internal table. Otherwise, continue.
5. Replace the source IP address of the DNS request with the Prestige's own WAN IP address and forward this new DNS request to the ISP DNS server.
6. Match the DNS response from the ISP DNS server to the original DNS request in the internal table. Replace the destination IP address of the DNS response with the original client's IP address and forward this new DNS response to the original client.

Nailed-up Connection

When enabled in a remote node configuration, this node will emulate a leased line connection, even though the physical line is a dial-up connection. The Prestige will dial and hold up a connection, without any traffic requesting it. A new option marked in **black** on the following menus, enables/disables this feature

Menu 11.1:

```
              Menu 11.1 - Remote Node Profile
     Rem Node Name= abc
     Active= Yes                                  Route= IP
     Call Direction= Outgoing             Bridge= No
     Tunneling Mode= None
       Endpoint Index= N/A                 Edit PPP Options= No
                                                      Rem IP Addr= 0.0.0.0
     Incoming:                                      Edit IP/IPX/Bridge= No
       Rem Login= N/A                      Telco Option:
       Rem Password= N/A                   Allocated Budget(min)= 0
       Rem CLID= N/A                           Period(hr)= 0
       Call Back= N/A                         Transfer Type= 64K
     Outgoing:                                Nailed-Up Connection= No
       My Login= scci                      Session Options:
       My Password= ********               Edit Filter Sets= No
       Authen= CHAP/PAP                    Idle Timeout(sec)= 300
       Pri Phone #= 140812345678
       Sec Phone #= 140822345678
                   Press ENTER to Confirm or ESC to Cancel:
```

Nailed-up Function Notes:

Because only two B-channels are available for the 8/12 remote nodes, the Prestige **always** starts to dial the first two remote nodes with the nailed-up connection requirement.

If it fails to establish a nailed-up connection (i.e. the call does not complete, or the session does not authenticate), the Prestige will keep attempting to connect to the same remote node, until the connection succeeds or exceeds the value set in ***Retry Counter*** field in Menu 24.9.1. This remote node is still under the budget control set in ***Allocated Budget*** and ***Period*** fields under ***Telco Option*** in Menu 11.1.

A remote node set as a nailed-up connection has no priority over any other remote nodes, except it keeps attempting until the connection succeeds. In other words, it is possible that other remote node connections may be established before the nailed-up connections. (i. e. -- First come, first serve.)

If a nailed-up connection is manually dropped, or lost from a line interruption, it will redial to reestablish the connection. But as above, it may fail if another other connection has already occupied the channel(s).

No idle timeout applies to nailed-up connections.

MP configuration is allowed to a nailed-up remote node. Each link of the MP will compete for the B-channel resources with other nailed-up or non-nailed-up remote node -- again first come, first serve.

Backup and Restore Configuration File via LAN or WAN

With the stand-alone Java based utility, PCT (Prestige Configuration Transfer), you can backup and restore your configuration file via LAN or WAN. Please refer to the PCT release notes for more information.

Upgrade P128IMH Firmware via LAN

With PCT, you can upgrade P128IMH firmware over the local LAN. (Attempting to upgrade a remote Prestige via the ISDN WAN is **not** recommended, even though it may succeed.). Please refer to PCT release notes for more information.

CI Commands

Here is the brief description about the most frequently used CI commands. The sequence of the following table is based on the commands' alphabetic order.

CI Command	brief description
bridge stat disp	statistics on Bridge packets
bridge blt disp	Bridge LAN table
bridge brt disp	Bridge WAN table
dev channel disp [bri0 | bri1]	show channel information on bri0 or bri1
dev channel drop [bri0 | bri1]	drop channel bri0 or bri1
dev dial x	manually dial to remote node x; x is the remote node number here
ether config	show the current Ethernet configuration
ether driver cnt disp	statistics on the Ethernet driver
Exit	exit from CI mode
ip address	LAN IP address
ip ping {IP address}	Ping {IP address}
ip route stat	IP routing table
ip status	statistics on IP packets
ip sua iface [wanif0 | wanif1] disp	display the SUA table for iface wanif0 or wanif1
ipx route stat	IPX routing table
ipx sap stat	IPX SAP table
isdn atring clear [bri0 | bri1]	clear the ISDN ring buffer of bri0 or bri1
isdn atring disp [bri0 | bri1]	display the ISDN ring buffer of bri0 or bri1
isdn config	show the current ISDN configuration
isdn fw ana dump	display ISDN trace messages on screen
isdn fw ana [on | off]	enable/disable ISDN trace

	mechanism
Isdn fw cnt disp	display ISDN transmission counters
isdn initstring clear	clear ISDN init string
isdn initstring set {at commands}	set ISDN init string to {at commands}
isdn reset	initialize the ISDN line
ppp lcp acfc [on | off]	enable/disable PPP LCP ACFC negotiation
ppp lcp bacp [on | off]	enable/disable PPP LCP BACP negotiation
ppp lcp callback [on | off]	enable/disable PPP LCP Microsoft callback negotiation
ppp lcp pfc [on | off]	enable/disable PPP LCP PFC negotiation
sys countrycode x	set country code
sys trcl call	show call trace on the screen
sys log disp	display the error/warning/information messages in the system log
sys log clear	clear the existing contents in system log
sys mbuf pool	display the pool of mbuf; mbuf is the buffer pre-allocated for data transmission
sys mbuf status	display mbuf status
sys memutil mqueue	statistics on pre-allocated system memory cell
sys memutil usage	statistics on the memory utilization
sys stdio 0	set SMT session timeout value to 0 –> never timeout
sys trcd	display the packet trace on screen
sys trcl clear	clear the existing contents in logic trace log
sys trcl disp	display the contents in both of logic and packet trace logs
sys trcl switch [on|off]	enable/disable logic trace log mechanism
sys trcp chann [in|out|both|enet0]	Enable the packet trace mechanism on incoming, outgoing, or both from WAN; or from Ethernet.
sys trcp disp	display the contents in packet trace log
sys trcp switch [on|off]	enable/disable packet trace log mechanism

Known Problem List

1. If Prestige connects to the switch that does not support in-band tone, the tone will generated by Prestige instead. In this case, Prestige will send the same tone to both POTS ports. For example, when telephone 1(telephone connects to POTS port 1) is ringing, off-hooking telephone 2 (telephone connects to POTS port 2) will cause telephone 1's sound changing from ring to dial tone. It is because Prestige generates dial tone for POTS port 2 now.
2. For DSS-1 version, a global digital call will still ring and can be answered even if **MSN** is selected in Menu 2 as the ***incoming call matching*** method.
3. The POTS port (A/B adapter) dial tone may disappear if call bumping is attempted twice in rapid succession on a switch that does not support in-band tone.
4. For DSS-1 version, the ISDN ***Link*** status still shows **Idle** in Menu 24.1 even if the cable is unplugged.
5. For DSS-1 version, Prestige may stop placing outgoing data calls after Call Waiting/Call Hold/ Call Retrieve scenario if both of POTS ports are assigned the identical phone number. When it happens, the B-channel status shown on Menu 24.1 is wrong.
6. Prestige performance will be degraded if there exists a telnet session in Menu 24.1 via LAN at the same time.
7. Select Nail-up Connection to Yes, and save it, next select Nail-up Connection to No, the Idle timeout will be change to 0, not the default value 300.
8. Make two seperated data connection, offhook A/B adapter will get busy tone and noise.
9. Make a modem connection, then change menu 2 B channel usage and save it, Prestige will hang about 20 seconds.
10. The feature of modem login script will be enhanced at next incremental release.
11. The CLID display service is not available for UK.
12. The modem firmware upgrade will take 10 minutes, a enhance will make it shorter.

To Get Prestige 128IMH

Get the files from ZyXEL anonymous FTP server (ftp.zyxel.com). Upgrade your Prestige by following the instructions for your model:

P128IMH

Versions:
RAS S/W Version - V2.21 | 18/01/99
ISDN F/W Version - DSS1: V 09a

RAS and ISDN firmware files:
p128imhe.bin (for DSS1)

Commands:
ATBAx: Where x = baud rate
options available are:
1= 38.4K
2= 19.2K
3= 9.6K
4= 57.6K
5= 115.2K
ATUR: Upload Firmware file via XMODEM

Romfile: romfile.zip (p128imh.rom)
ATUR3: Upload Romfile and clear all settings, the setting will change to manufactory setting, baud rate sets to 9.6K, please change to 9.6K for further configuration.

FAQ

Read by PDF

Read by Web Browser

ZyXEL Prestige 128IMH Router FAQ

General FAQ:

Specific FAQ:

---

19. What are supplemental services?
    19.a. Can I do call waiting?
    19.b. How do I do call waiting/Call Hold/Call Retrieve?
    19.c. Why Call Waiting does not work as expected?
    19.d. Can I do Conference Call?
    19.e. How do I do Conference Call?
    19.f. How do I remove a party from Three Way Calling?
    19.g. How do I do Call Transfer?
    19.h. How do I do blind Call Transfer?
    19.i. What is Call Forwarding and how do I do it?
    19.j. Why doesn't my answering machine on the POTS port stop recording?
20. What are CLIP and CLIR in Advanced Setup of Menu 2 (European firmware)?
21. Does ZyNOS support IRC, RealAudio, and CU-SeeME?
22. What do the errors mean?

General FAQ:

Q1: What are the differences between the Prestige 128IMH and Prestige 2864I?
A1: Compared to the Prestige 2864I, the Prestige 128IMH has two POTS ports with supplemental phone services, a built-in 4-port hub, and a 56K modem. Regarding the ISDN protocol, the P128IMH supports PPP only. For details, please refer to the following comparison chart (Table 1).

Table 1

Feature	P128IMH	P2864I
Physical Features		
UTP 10BaseT	Y	Y
AUI 10Base5	N	Y
POTS Port	2	1
Built-in Ethernet Hub	A built-in 4-port hub	N
Protocol Support		
IP	Y	Y
IPX	Y	Y
Transparent Bridging	Y	Y
PPP	Y	Y

RIP-2	Y	Y
SUA/NAT	Y	Y
WAN Capability		
ISDN Interface	BRI S/T and U	BRI S/T and U
ISDN B Channel Protocol	PPP only	PPP, V.120, X.75
ISDN Supplemental Phone Service	Y	N
ISDN Leased Line	Y	Y
Built-in Modem Capability	V.90 56Kbps	V.34 28.8Kbps
Bandwidth Optimization		
Dial on Demand	Y	Y
PPP/MP	Y	Y
BACP/BAP	Y	Y
Call Bumping	Y	Y
STAC Compression	Y	Y
Spoofing	Y	Y
Management		
Menu Driven Setup Interface	Y	Y
Prestige Web Configurator Support	Y	Y
Telnet In-Band Management	Y	Y
Console Port Out-of-Band Management	Y	Y
SNMP Management	Y	Y
Call Control	Y	Y
CDR(Call Detail Record)	Y	Y
Call History Support	Y	Y
Built-in Diagnostic Tool	Y	Y
Security		
PAP&CHAP	Y	Y

MS-CHAP	Y	Y
Call Back	Y	Y
Packet Filtering	Y	Y
RADIUS Client	Y	Y
CLID (Calling Line Identification)	Y	Y
Other Features		
DHCP Server	Y	Y
Dynamic/Static IP assignment	Y	Y
Multiple Signal User Account	Y	Y
Remote Node/Dial-in User number	12/8	12/8
Number of Client	Unlimited	Unlimited

Q2: What networking protocols does the Prestige 128IMH support?
A2: Prestige 128IMH supports TCP/IP, Novell IPX and Transparent Bridging (Table 1).

Q3: What WAN capability does the Prestige 128IMH support?
A3: Prestige 128IMH supports ISDN BRI (S/T and U interfaces) with PPP protocol. It also has a built-in V.90 client modem. This enables P128IMH to communicate with a 56K server at speeds of up to 56K through its ISDN interface. (Table 1)

Q4: What are the major applications for the Prestige 128IMH?
A4: The applications for P128IMH include Internet Access, Internet Signal User Account, LAN-to-LAN connection and Telecommuting server.

Q5: What supplemental phone services does the Prestige 128IMH support?
A5: Prestige 128IMH supports the following supplemental phone services on both POTS ports:

- Call Waiting
- Three-way Conference
- Call Transfer
- Call Forwarding
- Reminder Ring

Q6: What network management features does the Prestige 128IMH support?
A6: The Prestige 128IMH supports two methods of system management:

- SMT via the console port (or telnet)
- ZyXEL PWC tool

Q7: What data compression protocol does the Prestige support?
A7: The Prestige supports STAC compression and the built-in 56K modem supports V.42bis compression. Please note that STAC is not enabled in Prestige by default, but you can enable it in Remote Node setup (SMT menu 11.2, Edit PPP Option). The V.42bis is enabled in the built-in 56K modem by default.

Q8: What is ZyNOS?
A8: ZyNOS is the new Prestige router operating system. It is modular in design and so it is easy for developers to add features for different Prestige models. ZyNOS starts with firmware version number V2.xx. ZyNOS is available for Prestige 128IMH already, and will be available for:

P100MH, P100WH, P128MH, P153, P153X, P100, P100IH, P128 Plus

Only the old models of P128 and P2864I can't support ZyNOS because of limited Flash-EPROM and DRAM size.

Specific FAQ:

Q1: How do I access the Prestige SMT menu?
A1: The SMT interface is menu driven, which can be accessed via a RS232 console or a Telnet connection. To access the Prestige via SMT console port, a computer equipped with communication software such as HyperTerminal must be configured to the following parameters.

- VT100 terminal emulation
- 9600bps baud rate
- N81 data format (No Parity, 8 data bits, 1 stop bit)

The default console port baud rate is 9600bps - you can change it to 115200bps in menu 24.2.2 to speed up access of the SMT.

Q2: How do I upload ZyNOS code?
A2: There are two ways to upload the ZyNOS code to the Prestige. You can use PCT to install the code via LAN or use the console port to install the code via RS232.

The procedure for uploading ZyNOS via the console port is as follows.

- Enter debug mode when powering on the Prestige using a terminal emulator
- Type ATUR to start the uploading
- Use X-modem protocol to transfer the RAS code
- Type ATGO to restart the Prestige

Q3: How do I upload ROMFILE?
A3: In some situations, you may need to upload the ROMFILE, such as if you lose the system password, or if you need to reset the SMT to the factory defaults. There are three ways to upload the ROMFILE:

- use AT command: atur3
- use SMT Menu 24.6
- use TFTP/PCT

The procedure for uploading via the console port with ATUR3 command is as follows.

- Enter debug mode when powering on the Prestige using a terminal emulator
- Type ATUR3 to start the uploading
- Use X-modem protocol to transfer ROMFILE
- Enter ATGO to restart the Prestige

The PCT (Prestige Configuration Tool), a stand-alone Java-based utility which uses TFTP to allow the backup and restoration of the configuration file via LAN or WAN. Please note that other pure TFTP programs can not upload SMT configurations. A pure TFTP can not make the configuration parameters consistent within the ROMFILE. Inconsistencies among parameters in the ROMFILE may cause problems when you access the SMT.

Q4: What should I do if I forget the system password?
A4: If you forget the system password, you need to upload the ROMFILE to reset

the SMT to factory default. After the ROMFILE is uploaded, the default system password will be **"1234".**

Q5: Why do we need input filter menu 3.1 and call filter menu 11.1?
A5: Two factory default filter sets have been optimized for Internet connection. They are configured in menu 21 and applied to menu 3.1 and menu 11.5 to Prevent NETBIOS triggering the call. You certainly can remove it if you do not need it.

Q6: Why does the connection always drop after about 5 minutes when dialing to the Prestige using Win95 Dial-up Networking?
A6: Because Win95 Dial-up Networking is unable to respond to the CHAP challenges from the Prestige after the PPP connection is established, the **"Recv. Authen"** option (in Menu 13, "PPP Options) should be set to '**PAP**' only.

Q7: Can I apply the CLID Authentication?
A7: Because CLID (Calling Line Identification) is sent by the switch, CLID authentication is switch-dependent. If the switch supports Caller ID you can apply CLID authentication to the Prestige.

Q8: What is SUA? When should I use SUA?
A8: SUA (Single User Account) is a unique feature supported by the Prestige router which allows more than 1 person to access the Internet concurrently for the cost of a single user account.

Most ISPs offer two types of service:

- A class C address account
- A single user account

A Class C address account allows a company with up to 255 workstations to access the Internet concurrently, while a single user account only allows one user to access the Internet. The service charges for a Class C address account is typically much higher than that for a single user account.

Q9: What is the difference between NAT and SUA?
A9: NAT is a generic name defined in RFC 1631, the **"IP Network Address Translator (NAT)"** SUA (Internet Single User Account) is ZyXEL'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 find themselves unable to connect to the Internet.

Basically, NAT is a process of translating one address to another. NAT implementation can be as simply 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 ZyXEL'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.

Q10: How many network users can the SUA support?
A10: The fixed-size translation table limits the number of simultaneous attempts to access the Internet. A reasonable number will be less than 20 users. Beyond that, the limited modem bandwidth would probably become the bottleneck and any increase in the translation table size would not help.

Q11: How do I capture the PPP log in my Prestige?
A11: The procedure to capture the PPP log in the Prestige is as follows.

To enable the capture of PPP log before a connection is established:

- go to SMT Menu 24.8, and enter CI command mode
- enter **"sys trcl cl"**
- enter **"sys trcl sw on"**
- enter **"sys trcp sw on"**

To display the PPP log after a connection is disconnected:

- enter **"sys trcl sw off"** command
- enter **"sys trcp sw off"** command
- enter **"sys trcl disp"** command

Q12: Why can’t I make a voice call via the a/b adapter 2 when the internal modem is up and running?

A12: When the internal modem is disabled, the two POTS ports on P128IMH router can be used at the same time. When the internal modem is enabled, only a/b adapter 1 is available for communications.

Q13: What is DNX proxy?
A13: If enabled, DNS Proxy will allow the Prestige to act as the DNS server for the local network. The Prestige will get the IP address of the actual DNS server from the remote site via IPCP negotiation. Note this feature only works if the remote site supports RFC 1877.

Q13.a: How do I enable DNS proxy?
A13.a: DNS Proxy is enabled only if the selection of the DHCP field under DHCP Setup in Menu 3.2 is Server and the Primary DNS Server field in Menu 3.2 is set to 0.0.0.0. (this is the factory default). If the DNS Proxy is enabled, the Prestige will assign its IP address as the Primary DNS in response to DHCP requests on the local network.

Q13.b: How do I set DNS other than Prestige's IP address?
A13.b: If the DNS is already known to you, you can enter it in the Primary DNS server and Secondary DNS server fields in Menu 3.2 to respond to the DHCP requests on the local network if DHCP Server function is enabled.

Q14: What is a Nailed-up Connection and when do I need to use it?
A14: A Nailed-up Connection, when enabled, will emulate a leased line connection even though the physical line is a dial-up connection. The Prestige will dial and hold up a connection, without any traffic requesting it. When you want the link to be always up, you need to use it.

Q15: What are device filters and protocol filters?
A15: In ZyNOS, the filters have been separated into two groups. One is called the device filter group, and the other is called the protocol filter group. Generic filters belong to the device filter group, TCP/IP and IPX filters belong to the protocol filter group.

Q16: Why can’t I configure device filters or protocol filters?
A16: Because in ZyNOS, you can not mix different filter groups in the same filter set.

Q17: How can my client connect to my server via a Prestige that supports SUA?
A17: You need to configure Menu 15 SUA - Server Setup. Enter the port number if

you know it, e.g. port 21 for FTP server, and then enter the IP address of this FTP server. The remote clients can then access the FTP serve by using Prestige's Internet address (WAN IP).

Q18: How does 'Dial Prefix to Access Outside Line' in Menu 2 (European firmware) work?
A18: This is the number that will be placed in front of the outgoing call phone numbers when you make an outgoing call.

Q19: What are supplemental services?
A19: ISDN Supplemental Services refers to Call Waiting/Call Hold/Call Retrieve, Three-way Calling (Conference/Transfer/Drop), Call Forwarding, and Reminder Ring on the Prestige POTS ports. There are services on the serving Central Office switch that works in tandem with the Prestige software which must be enabled.

19.a. Can I do call waiting?

Yes. You need to subscribe to Additional Call Offering (ACO) (in Europe the same service is better known as “Call Waiting”) on your ISDN line in order to utilize the Call Waiting/Call Hold/Call Retrieve feature.

19.b. How do I do call waiting/Call Hold/Call Retrieve?

- Put your current call on hold and answer the incoming call – after hearing the call waiting tone, press and immediately release the flash button on your telephone.
- Put your current call on hold and switch to another call – press and immediately release the flash button on your telephone.
- Hang up your current call before answering the incoming call – hang up the phone and wait for the phone to ring. Then answer the incoming call.
- Hang up the current active call and switch back to the other call – hang up the phone and wait for the phone to ring. Then pick up the phone to return to the other call.

19.c. Why does Call Waiting not work as expected?

An incoming caller will receive a busy signal if:

- You have two calls (one active and one on hold; or both active by using Three Way Calling) on the Directory (Phone) number the incoming caller is attempting to reach.
- You are dialing out by using the Directory (Phone) number the incoming caller is attempting to reach, but have not yet established a connection.

If no action is taken to answer the call (call waiting indicator tone is ignored), the call waiting tones will disappear after about 20 seconds.

19.d. Can I do Conference Calls?

Yes. The Three Way Calling (Conference/Transfer/Drop) feature requires flexible calling on your ISDN line. You may want to check with your PTT to confirm if these services are available to you.

19.e. How do I do Conference Calls?

Press the flash button and immediately release it to put the existing call on hold and receive a dial tone.

- Dial the third party.
- Inform the third party about the conference.
- When you are ready to conference the call, press the flash hook button and immediately release it to establish a three-way Conference Call.

19.f. How do I remove a party from the three-way Calling?

If you wish to drop the last call added to a three-way Calling call, just press the flash key.
If you wish to drop yourself from the conference call, but allow the other two callers to remain connected, just hang up your phone. If the other two remain on line, your hanging up will not affect their connection.

19.g. How do I do Call Transfer?

Call Transfer is a variance of three-way Calling and allows you to transfer an active call to a third party. If you wish to transfer an active call to a third party and inform him about the transferred call, the steps are:

- Press flash to immediately put the existing call on hold and receive a dial tone
- Dial the third party
- Inform the third party about the transfer call
- Press the flash button and immediately release it to establish a three-way Conference Call
- Hang up the phone to complete the transfer

19.h. How do I do blind Call Transfer?

- Press flash to immediately put the existing call on hold and receive a dial tone
- Dial the third party
- Before the third party picks up the call, you can transfer the call by pressing the flash and hanging up.

The call will be automatically transferred.

19.i. What is Call Forwarding and how do I do it?

Call Forwarding feature is supported by ISDN switch directly. The Call Forwarding feature of the POTS port can be activated and deactivated by using the phone set. Please request your telecom for the instructions to activate or deactivate the Call Forwarding feature.

19.j. Why doesn't my answering machine on the POTS port stop recording?

Answer machine will stop record when it receives busy tone or detects a period time of silence. If your POTS will connect to answer machine, you need set S78.5 and S78.6 to set the silence time. When it sets to 5 sec, Prestige will be silent 5 sec after remote hangs up, and then produces busy tone. Since most of the answer machines detect busy tone, so the default is 0 sec. If you have an answer machine detecting silence, you need set the s78.5 s78.6 to meet your need. This should be added at initstring by the following CI command.

isdn init set s78.6=0s78.5=1

S78.6	S78.5	silence time
0	0	0 sec
0	1	5 sec
1	0	10 sec
1	1	15 sec

Q20: What are CLIP and CLIR in Advanced Setup of Menu 2 (European firmware)?
A20: The CLIP or CLIR refers to CLID Presented or Restricted The Prestige can set the CLIP/CLIR bit in the SETUP message to request the Switch to include calling party number or not when the switch sends the SETUP message to the called party. Therefore, before using it you need to subscribe to it first from your telecom as a supplemental service.

Q21: Does ZyNOS support IRC, RealAudio, and CU-SeeME?
A21: Yes. IRC, which is an Internet Chat service like NetMeeting, is supported in SUA mode. RealAudio and CU-SeeMe are also supported.

Q22: What do the errors mean?
A22: The meanings of some codes are as follow.

-3000 === remote node is connecting
-3001 === configured incoming call only, outgoing call fails
-3002 === configured outgoing call only, incoming call fails
-3003 === packet is filtered
-3004 === no iface
-3005 === no channel available
-3006 === call request fail
-3007 === remote node is waiting call back
-3020 === call dial fail
-3022 === filter groups are mixed, so call is not allowed
-3023 === received unexpected event
-3024 === state timeout
-3025 === waiting RADIUS authentication
-3026 === RADIUS call back fail
-3028 === the node is not found
-3029 === the node is inactive
-3030 === dial fail
-3031 === no budget
-3032 === radius authentication fail
-3033 === CLID is required

-3034 === CLID can not be found
-3035 === an outgoing call has already been placed for this remote node
-3036 === call is blocked
-3037 === invalid phone number
-3038 === remote side is busy
-3039 === no carrier
-3040 === no dial tone
-3041 === remote node is not active
-3042 === no answer received
-3043 === dial timeout
-3044 === redial no method
-3045 === redial stopped
-3046 === redial no number
-3047 === first call is CLID authenticated and remote node is obtained but ppp is not up yet, second call has same CLID
-3048 === remote node does not supported L2TP

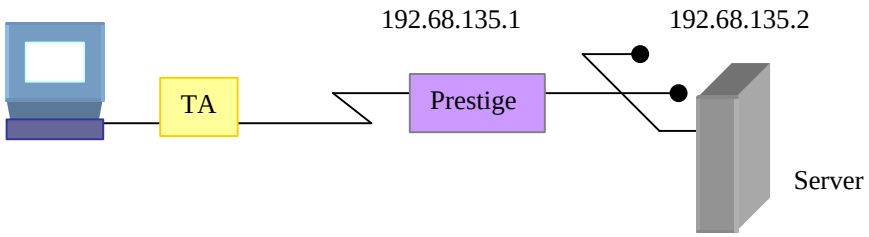
Telecommuting

Using an ISDN TA and Win9x Dial-Up Networking to dial into Prestige router with callback and without callback

➢ Introduction

This configuration note explains how to set up a workstation using an ISDN TA to connect to the Prestige router. In this configuration, the workstation must have TCP/IP dial-up program installed such as Windows Dial-up Networking to make the call. Once the connection is established, the workstation will be able to perform any TCP/IP applications (e.g., FTP, Telnet, etc.). There will be two items that you need to set up for this connection. They are the workstation and the Prestige router.

➢ Configuration



➢ Setting up the Win9x Dial-Up Networking

To set up the DUN for this connection, you will need to set the following parameters:

- ✓ *phone number*- the phone number of Prestige router
- ✓ *Internet account*-Username and Password
- ✓ *IP Address*-the IP address in this case will be dynamically assigned by the Prestige. Generally, you should simply enter '0.0.0.0' into the IP address field.
- ✓ *DNS (Domain Name Server) Address*- the IP address of the DNS server on the remote LAN.
- ✓ *Default Gateway*-the IP address of the Prestige

Please find the last three settings in **'Win9x>Dial-Up Networking>Properties>Server Types>TCPIP Settings'**.

➢ Setting up the Prestige

Before configuring the Prestige for this application, you need to complete the following settings first.

- ✓ *General Setup in SMT menu 1*-enter the system information.
- ✓ *ISDN Setup in SMT menu 2-enter your ISDN number*
- ✓ *Ethernet Setup in SMT menu 3*-enter the IP address of the Prestige and enable the DHCP server if it is required.

To setup the Prestige for this application, make sure you have the following menus configured correctly.

- ✓ *Default Dial-in Setup in SMT menu 13*
- ✓ *Edit Dial-in User in SMT menu 14*

1. Ethernet Setup in SMT Menu 3

```
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= 192.68.135.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-1
```

2. Default Dial-in Setup in SMT Menu 13

```
Menu 13 - Default Dial-in Setup

Telco Options:                  IP Address Supplied By:
  CLID Authen= None               Dial-in User= No
                                  IP Pool= Yes
PPP Options:                    IP Start Addr= 192.68.135.10
  Recv Authen= PAP                IP Count(1,2)= 2
  Compression= Yes
  Mutual Authen= No             IPX Net Num Supplied By:
    PAP Login= N/A              IPX Pool= No
    PAP Password= N/A             IPX Start Net Num= N/A
  Multiple Link Options:          IPX Count(2,16)= N/A
    Max Trans Rate(Kbps)= 128
                                Session Options:
Callback Budget Management:       Edit Filter Sets= No
  Allocated Budget(min)=          Idle Timeout= 300
  Period(hr)=

          Press ENTER to Confirm or ESC to Cancel:
```

* The **Recv Authen** field should be set to the type of authentication protocol you want to use.
* Since the workstation needs to have its IP address assigned, set the '**IP Address Supplied** By: Dial-in User' field to **'No'**.
* Make sure that **IP Pool** is set to **'Yes'**.
* In **IP Start Addr**, enter the IP address that you want to assign to the workstation when it dials in. In our example, this would be **'192.68.135.10'**.

All the common properties in Menu 13 will be applied to all dial-in users.

Note: If the remote user uses the Win9x to dial in, the 'Recv Authen' must be set to 'PAP' because Dial-up Networking V1.1 will not response to any periodic CHAP challenge sent by Prestige and will causes Prestige to drop the call.

3. Edit Dial-in User Setup in SMT menu 14

```
Menu 14 - Dial-in User Setup

1. abc
2. _________
3. _________
4. _________
5. _________
6. _________
7. _________
8. _________
```

➢ Dial-in user without callback

```
Menu 14.1 - Edit Dial-in User

User Name= abc
Active= Yes
Password= ********
Callback= No
  Phone # Supplied by Caller= N/A
  Callback Phone #= N/A
Rem CLID=
Idle Timeout= 300
```

* The User Name and Password fields should be set to the login username and password that the workstation will provide when dialing in to Prestige.
* Set the Active field to **'Yes'**

➢ Dial-in user with callback

```
Menu 14.1 - Edit Dial-in User

User Name= ABC
Active= Yes
Password= ********
Callback= Mandatory
  Phone # Supplied by Caller= Yes
  Callback Phone #= N/A
Rem CLID=
Idle Timeout= 300
```

There are two options for the callback, **'Mandatory'** and **'Optional'**. If the Mandatory is configured, the Prestige router has to callback anyway. If the Optional is configured, the dial-in user will have the chance to cancel the callback.
The number for calling back to the dial-in user can be specified by user during the connection or pre-configured in the **'Callback Phone #'** field of Prestige.

Internet Connection

Internet Connection without SUA

Internet Connection with SUA

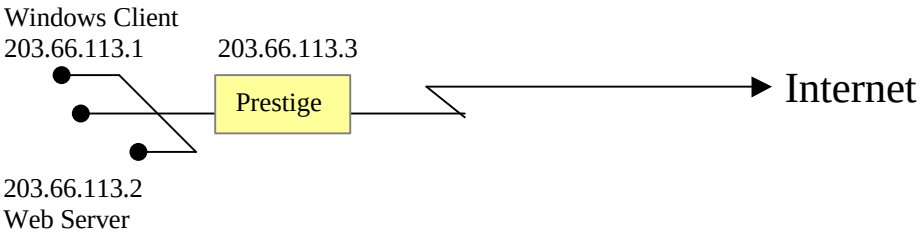
Internet Access

Internet Access for Workstation/PC where ISP assigns a static Class C address

➢ Introduction

This configuration note explains how to set up the workstation and the Prestige to connect to the Internet via ISP. In this configuration, the user has a class C Internet account that will assign a static IP address. There will be two items that you need to set up. These are workstation and the Prestige router.

➢ Configuration



➢ Setting up the Win9x Workstation

To set up the workstation, you will need to set the following parameters:

- ✓ *IP Address*-the IP address assigned to the workstation itself
- ✓ *Subnet Mask*-the subnet mask used for your network. A Class C network generally uses a 24-bit netmask, 255.255.255.0.
- ✓ *DNS (Domain Name Server) Address-enter the ISP's DNS or your DNS on the local LAN.*
- ✓ *Default Gateway*-the IP address of the Prestige

For Windows Client, please go to ***Win9x>Control Panel>Network>TCPIP-Network Adapter*** for finishing the above settings.

➢ Setting up the Prestige

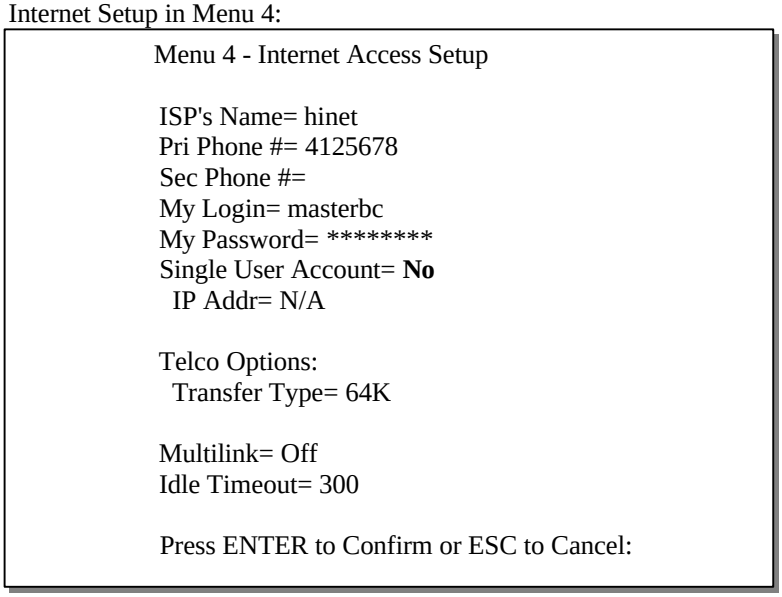
Before configuring the ISP account in Prestige, you need to complete the following settings in Prestige first.

- ✓ *General Setup in SMT menu 1*-enter the system information.
- ✓ *ISDN Setup in SMT menu 2-enter* your ISDN number
- ✓ *Ethernet Setup in SMT menu 3*-enter the IP address of the Prestige and enable the DHCP server if it is required.

To setup the Prestige for Internet access (SMT Menu 4), you need to get the following information from your ISP:

- ✓ *ISP phone number*
- ✓ *Internet account*-Username and Password

Internet Setup in Menu 4:



* Since you have a Class C Internet account, Single User Account should be set to **'No'**.
After saving this menu, you will be asked if you want to perform an Internet connection test. Select **'Yes'** to perform the test. If the test fails, please check again the above settings or refer to the User's Manual Troubleshooting section for correction action.

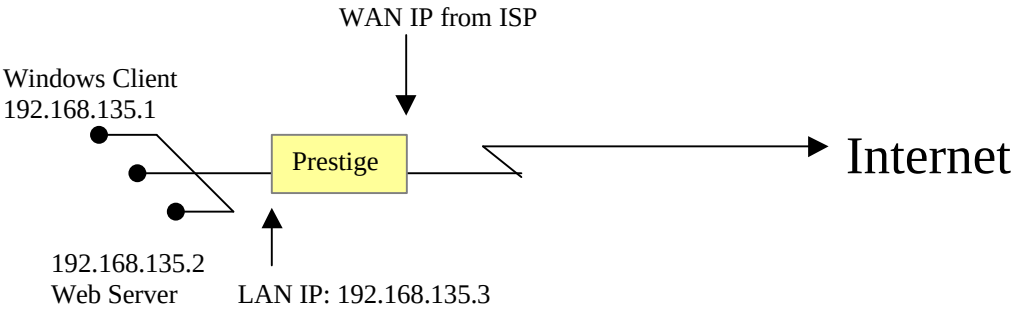
Internet Access

Configuring Prestige for Internet access with SUA **(Single User Account)**

➢ Introduction

This configuration note explains how to set up a workstation and the Prestige to connect to the Internet via ISP. In this configuration, the user has a single user Internet account that will assign one IP address dynamically. Notice that with this configuration, all stations on the network will be able to access the Internet, but they will be hidden from outsides. That is, from the ISP's point of view, they will only be able to see the single IP address (in this case, the one dynamically assigned). There will be two items that you need to set up. These are workstation and the Prestige router.

➢ Configuration



➢ Setting up the Win9x Workstation

To set up the workstation, you will need to set the following parameters:

- ✓ *IP Address*-the IP address assigned to the workstation itself
- ✓ *Subnet Mask*-the subnet mask used for your network. A Class C networks generally uses a 24-bit netmask, 255.255.255.0.
- ✓ *DNS (Domain Name Server) Address-enter the ISP's DNS or your DNS on the local LAN.*
- ✓ *Default Gateway*-the IP address of the Prestige

[Please go to ***Win9x>Control Panel>Network>TCPIP-Network Adapter*** for finishing the above settings.]

➢ Setting up the Prestige router

Before configuring the ISP account in Prestige, you need to complete the following settings in Prestige first.

- ✓ *General Setup in SMT Menu 1*-enter the system information.
- ✓ *ISDN Setup in SMT Menu 2*-configure the ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-enter the IP address of Prestige, and enable the DHCP server if it is required.

To setup the Prestige Internet access (SMT Menu 4), you need to get the following information from your ISP:

- ✓ *ISP phone number*

- ✓ *Internet account*-Username and Password

Internet Access Setup in SMT Menu 4:

```
                Menu 4 - Internet Access Setup

                ISP's Name= hinet
                Pri Phone #= 4125678
                Sec Phone #=
                My Login= masterbc
                My Password= ********
                Single User Account= Yes
                  IP Addr= 0.0.0.0

                Telco Options:
                  Transfer Type= 64K

                Multilink= Off
                Idle Timeout= 300
                Press ENTER to Confirm or ESC to Cancel:
```

* **Pri Phone#=** is the phone number your Prestige has to dial in order to access your ISP.
* **My Login** and **My Password** are the login information provided by ISP.
* Since you have a single user Internet account**, Single User Account** should be set to **'Yes'**.
* For the **Local IP Address** field, since the IP address will be dynamically assigned, either **'0.0.0.0'** or you can leave this field blank

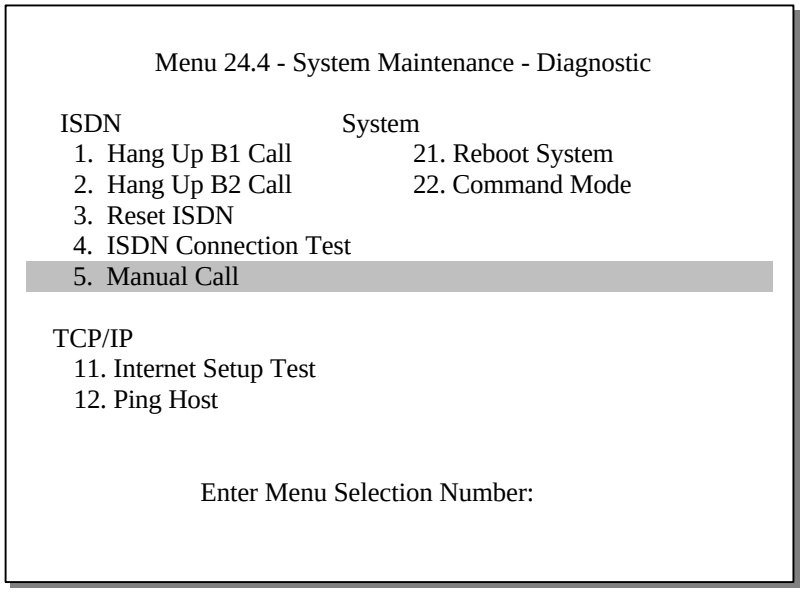
After saving this menu, you will be asked if you want to perform an Internet connection test. Select **'Yes'** to perform the test. If the test fails, please check again the above settings or refer to the User's Manual Troubleshooting section for correction action.

When you have configured and saved Menu 4, you should see that you have created a remote node in Menu 11. You can perform more advanced configuration options to this remote node in this menu.

```
Menu 11 - Remote Node Setup

        1. hinet (ISP)
        2. _________
        3. _________
        4. _________
```

```
                Menu 11.1 - Remote Node Profile

Rem Node Name= hinet            Edit PPP Options= No
Active= Yes                     Rem IP Addr= 0.0.0.0
Call Direction= Outgoing        Edit IP= No
                                Edit Script Options= No
Incoming:
  Rem Login=                    Telco Option:
  Rem Password= ********        Allocated Budget(min)= 0
  Rem CLID= N/A                 Period(hr)= 0
  Call Back= N/A
Outgoing:                       Session Options:
  My Login= kib73820              Input Filter Sets=
  My Password= ********           Output Filter Sets=
  Authen= CHAP/PAP                Call Filter Sets=
  Pri Phone #= 0,5007025        Idle Timeout(sec)= 300
  Sec Phone #=

                Press ENTER to Confirm or ESC to Cancel:
```

In addition, you can make manual calls to the Internet by using the **'Manual Call'** or **'Internet Setup Test'** option in Menu 24.4 and selecting the corresponding 'ISP' remote node.



Configuring an Internal Server Behind SUA

➢ Introduction

If you wish, you can make internal servers (e.g., Web, ftp or mail server) accessible for outside users, even though SUA makes your LAN appear as a single machine to the outside world. A service is identified by the port number. Also, since you need to specify the IP address of a server in the Prestige, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

In addition to the servers for specific services, SUA supports a default server. A service requset that does not have a server explicitly designated for it is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

➢ Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server in **'Menu 15'**, Multiple Server Configuration.

✓ Example (Configuring an internal Web server for outside access)

Menu 15 - Multiple Server Configuration

	Port #	IP Address
1.	Default	0.0.0.0
2.	**80**	**192.168.135.2**
3.	0	0.0.0.0
4.	0	0.0.0.0
5.	0	0.0.0.0
6.	0	0.0.0.0
7.	0	0.0.0.0
8.	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

HTTP:80 FTP:21 TELNET:23 MAIL:25 PPTP:1723

✓ Port numbers for some services

Service	Port Number
FTP	21
telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80

LAN-to-LAN TCPIP Connection

Outgoing Connection

Incoming Connection

LAN-to-LAN via Two Prestige Routers

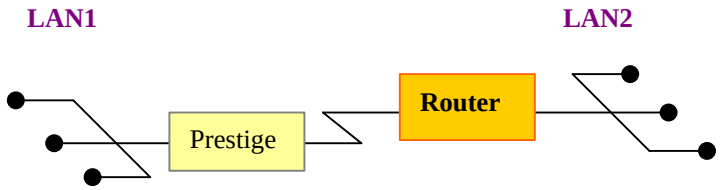
LAN-to-LAN Connection

Making a call to remote router for a LAN-to-LAN connection

➢ Introduction

This configuration note explains how to set up the Prestige to connect to remote router for a LAN-to-LAN connection. Once the connection is established, the workstations on both LANs will be able to perform any TCP/IP applications (e.g., FTP, Telnet, etc.). Before starting to configure the Prestige, please make sure all the configurations in the remote router are completed such as IP address, remote node setup, etc. After all, there will be two more items that you need to set up. These are workstation and the Prestige.

➢ Configuration



➢ Setting up the workstation on both LANs

To set up the workstations, you need to set the following parameters:

- ✓ *IP Address*-the IP address assigned to the workstation itself
- ✓ *Subnet Mask*-the subnet mask used for your network. A Class C network generally uses a 24-bit netmask, 255.255.255.0.
- ✓ *DNS (Domain Name Server) Address*-the ISP's DNS server or your local DNS server
- ✓ *Default Gateway*-the IP address of the station or device on your network that acts as a default gateway. That is, any packets without an implicit route to their destination IP address will be routed to the default gateway. The default gateway for LAN1 is Prestige router and for LAN2 is **'Router'**.

The procedure for configuring these parameters for the workstations may differ depending on the type of TCPIP networking software you are using on your workstations. If you are unfamiliar with how to set these parameters, you can refer to the technical notes corresponding to your software.

For Windows 9x, please go to ***'Win9x>Control Panel>Network>TCPIP-Network Adapter'*** for finishing the above settings.

➢ Setting up Prestige

Before configuring Prestige for this application, you need to complete the following settings first.

- ✓ *General Setup in SMT Menu 1*-enter the system information.
- ✓ *ISDN Setup in SMT Menu 2*- enter your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-enter the IP address of the Prestige and enable the DHCP server if it is required.
- ✓ *Remote Node Setup in SMT Menu 11*

To setup the Prestige for this LAN-to-LAN application, make sure you have the following menus configured correctly.

1. Ethernet Setup in SMT Menu 3

```
        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= 203.66.113.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= Both
        Version= RIP-2B
```

2. Remote Node Setup in SMT Menu 11

```
        Menu 11.1 - Remote Node Profile

Rem Node Name= LAN2          Route = IP
Active = Yes                 Bridge = No
                             Edit PPP Options = No
Call Direction = Outgoing    Rem IP Addr= 202.113.5.1
 Incoming:                   Edit IP/IPX/Bridge = No
  Rem Login=                 Telco Option:
  Rem Password=                Allocated Budget(min)= 0
  Rem CLID= N/A                 Period(hr)= 0
  Call Back= N/A
Outgoing:                    Session Options:
  My Login= test               Edit Filter Sets = No
  My Password= 1234             Idle Timeout(sec)= 300
  Authen= CHAP/PAP
  Pri Phone #= 5007025
  Sec Phone #=

          Press ENTER to Confirm or ESC to Cancel:
```

* Select the **'Active'** field to **'Yes'**
* Select the **'Call Direction'** to **'Outgoing'**
* Enter the correct **'My Login'** and **'My Password'** corresponding to the node account in remote router.
* Select the '**Authen'** type the remote router supports
* Enter the phone number of the remote router in the **'Pri Phone #'** field
* Enter the IP address of the remote router in **'Rem IP Addr'** field
* Enter the idle timer in the **'Idle Timeout'** field for dropping the call if there is no data traffic between the two nodes.

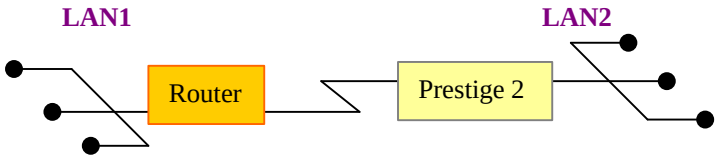
LAN-to-LAN Connection

Answering a call from a remote router for a LAN-to-LAN connection

➢ Introduction

This configuration note explains how to set up the Prestige to answer calls from the remote router for a LAN-to-LAN connection. Once the connection is established, the workstations on both LANs will be able to perform any TCP/IP applications (e.g., FTP, Telnet, etc.). Before starting to configure the Prestige, please make sure all the configurations in the remote router are completed such as IP address, remote node setup, etc. After all, there will be two more items that you need to set up. These are workstation and the Prestige.

➢ Configuration



➢ Setting up the workstation on both LANs

To set up the workstations, you will need to set the following parameters:

- ✓ *IP Address*-the IP address assigned to the workstation itself
- ✓ *Subnet Mask*-the subnet mask used for your network. Class C networks generally use a 24-bit netmask, 255.255.255.0.
- ✓ *DNS (Domain Name Server) Address*-the IP address of the server station on your network that acts as the DNS.
- ✓ *Default Gateway*-the IP address of the station or device on your network that acts as a default gateway. That is, any packets without an implicit route to their destination IP address will be routed to the default gateway. The default gateway for LAN1 is the 'Router' and for LAN2 is Prestige.

The procedure for configuring these parameters for the workstations may differ depending on the type of TCPIP networking software you are using on your workstations. If you are unfamiliar with how to set these parameters, you can refer to the technical notes corresponding to your software.

For Windows 9x, please go to ***'Win9x>Control Panel>Network>TCPIP-Network Adapter'*** for finishing the above settings.

➢ Setting up the Prestige router

Before configuring the Prestige for this application, you need to complete the following settings first.

- ✓ *General Setup in SMT Menu 1*-enter the system information.
- ✓ *ISDN Setup in SMT Menu 2*-Enter your ISDN number
- ✓ *Ethernet Setup in SMT menu 3*-enter the IP address of the Prestige and enable the DHCP server if it is required.

✓ To setup the Prestige for this LAN to LAN application, make sure you have the following menus configured correctly.

✓ *Remote Node Setup in SMT Menu 11*

1. Ethernet Setup in SMT Menu 3

```
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= 203.66.113.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

2. Remote Node Setup in SMT Menu 11

```
Menu 11.1 - Remote Node Profile

  Rem Node Name= LAN2          Route= IP
  Active= Yes                  Bridge= No

  Call Direction= Incoming     Edit PPP Options= No
  Incoming:                    Rem IP Addr= 202.113.5.1
    Rem Login= test            Edit IP/IPX/Bridge= No
    Rem Password= 1234          Telco Option:
    Rem CLID=                     Allocated Budget(min)= 0
    Call Back= N/A                Period(hr)= 0
  Outgoing:                       Transfer Type= 64K
    My Login=                     Nailed-Up Connection= N/A
    My Password= ********      Session Options:
    Authen= N/A                   Edit Filter Sets= No
    Pri Phone #= N/A              Idle Timeout(sec)= 300
    Sec Phone #= N/A

          Press ENTER to Confirm or ESC to Cancel:
```

* Select the **'Active'** field to **'Yes'**
* Select the **'Call Direction'** to **'Incoming'**
* Enter the correct node account in **'Rem Login'** and **'Rem Password'** fields
* Enter the IP address of the remote router in **'Rem IP Addr'** field

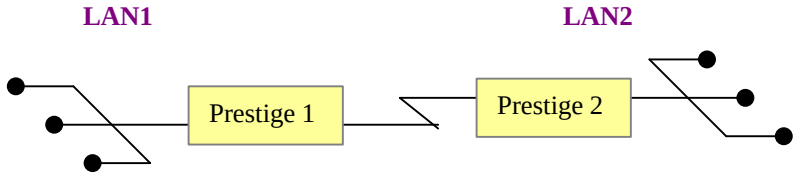
LAN-to-LAN TCPIP Connection

Connecting two LANs via Prestige routers for a TCPIP connection

➢ Introduction

This configuration note explains how to set up two Prestige routers for a LAN-to-LAN connection. Once the connection is established, the workstations on both LANs will be able to perform any TCP/IP applications (e.g., FTP, Telnet, etc.). There will be three items that you need to set up. These are workstation and the two Prestige routers.

➢ Configuration



➢ Setting up the workstation on both LANs

To set up the workstations, you will need to set the following parameters:

- ✓ *IP Address*-the IP address assigned to the workstation itself
- ✓ *Subnet Mask*-the subnet mask used for your network. Class C networks generally use a 24-bit netmask, '255.255.255.0'.
- ✓ *DNS (Domain Name Server) Address*-enter the IP address of the DNS server
- ✓ *Default Gateway*-the IP address of the Prestige, t***he default gateway for LAN1 is Prestige 1 and for LAN2 is Prestige 2.***

The procedure for configuring these parameters for the workstations may differ depending on the type of TCPIP networking software you are using on your workstations. If you are unfamiliar with how to set these parameters, you can refer to the technical notes corresponding to your software.

For Windows 9x, please go to 'Win9x>Control Panel>Network>TCPIP-Network Adapter' for finishing the above settings.

➢ Setting up the Prestige 1 & Prestige 2

Before configuring the two remote nodes for this application, you need to complete the following settings first in each Prestige.

- ✓ *General Setup in SMT Menu 1*-enter the system information.
- ✓ *ISDN Setup in SMT Menu 2*- Enter your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-enter the IP address of the Prestige and enable the DHCP server if it is required.

To setup the Prestige for this LAN to LAN connection, make sure you have the following menus configured correctly.

- ✓ *Remote Node Setup in SMT Menu 11*

➢ Prestige 1 Setup

1. Ethernet Setup in SMT Menu 3

```
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= 202.113.5.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

2. Remote Node Setup in SMT Menu 11

```
Menu 11.1 - Remote Node Profile

Rem Node Name= LAN2          Route = IP
Active = Yes                 Bridge = No
                             Edit PPP Options = No
Call Direction = Outgoing    Rem IP Addr= 203.66.113.1
 Incoming:                   Edit IP/IPX/Bridge = No
  Rem Login=                 Telco Option:
  Rem Password=                Allocated Budget(min)= 0
  Rem CLID= N/A                Period(hr)= 0
  Call Back= N/A
Outgoing:                    Session Options:
  My Login= test             Edit Filter Sets = No
  My Password= 1234          Idle Timeout(sec)= 300
  Authen= CHAP/PAP
  Pri Phone #= 5007025
  Sec Phone #=

        Press ENTER to Confirm or ESC to Cancel:
```

* Select the **'Active'** field to **'Yes'**
* Select the **'Call Direction'** to **'Outgoing'**
* Enter the correct node account in **'My Login'** and **'My Password'** fields
* Enter the phone number of the remote router in the **'Pri Phone #'** field
* Enter the IP address of the remote router in **'Rem IP Addr'** field
* Enter the idle timer in the **'Idle Timeout'** field for dropping the call if there is no data traffic between the two remote nodes

➢ Prestige 2 Setup

1. Ethernet Setup in SMT Menu 3

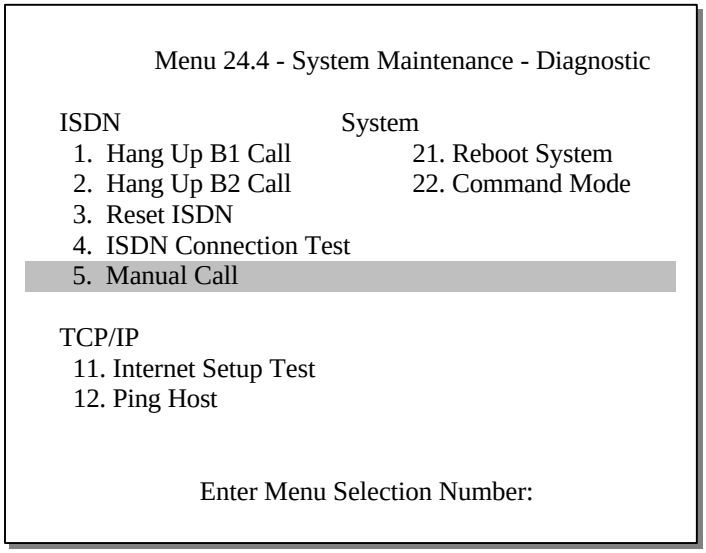
```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

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= 203.66.113.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

2. Remote Node Setup in SMT Menu 11

```
Menu 11.1 - Remote Node Profile

  Rem Node Name= LAN1          Route= IP
  Active= Yes                  Bridge= No

  Call Direction= Incoming     Edit PPP Options= No
  Incoming:                    Rem IP Addr= 202.113.5.1
    Rem Login= test            Edit IP/IPX/Bridge= No
    Rem Password= 1234          Telco Option:
    Rem CLID=                     Allocated Budget(min)= 0
    Call Back= N/A                Period(hr)= 0
  Outgoing:                       Transfer Type= 64K
    My Login=                     Nailed-Up Connection= N/A
    My Password= ********      Session Options:
    Authen= N/A                   Edit Filter Sets= No
    Pri Phone #= N/A              Idle Timeout(sec)= 300
    Sec Phone #= N/A

          Press ENTER to Confirm or ESC to Cancel:
```

* Select the **'Active'** field to **'Yes'**
* Select the **'Call Direction'** to **'Incoming'**
* Enter the correct node account for the dial-in router in **'Rem Login'** and **'Rem Password'** fields
* Enter the IP address of remote router in **'Rem IP Addr'** field.

After you have finished the above settings, you are ready to make a test for this connection from Menu 24.4.5 **'Manual Call'** by entering the node number.

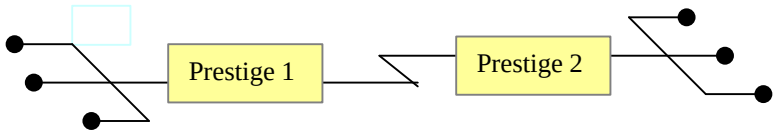


Bridge Configuration

➢ Introduction

This configuration note explains how to set up the bridging options for the Prestige router. Depending on your particular applications, you will need to configure different SMT Menus. We will illustrate the configuration for some applications in the following sections.

➢ Configuration



➢ Prestige 1 Setup

1. Enabling the **'Bridge'** option in SMT Menu 1

```
Menu 1 - General Setup

System Name= Prestige
Location= ZyXEL HQ
Contact Person's Name= abc

Route IP= No
Route IPX= No
Bridge= Yes
```

2. Ethernet Setup in SMT Menu 3

```
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= 202.113.5.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

3. Remote Node Setup in SMT Menu 11

```
Menu 11.1 - Remote Node Profile

  Rem Node Name= P2              Route= None
  Active= Yes                    Bridge= Yes

  Call Direction= Outgoing       Edit PPP Options= No
  Incoming:                      Rem IP Addr= N/A
    Rem Login=                   Edit IP/IPX/Bridge= Yes
    Rem Password=                Telco Option:
    Rem CLID=                      Allocated Budget(min)= 0
    Call Back= N/A                 Period(hr)= 0
  Outgoing:                        Transfer Type= 64K
    My Login=test                  Nailed-Up Connection= N/A
    My Password= 1234            Session Options:
    Authen= N/A                    Edit Filter Sets= No
    Pri Phone #= 5009097           Idle Timeout(sec)= 100
    Sec Phone #= N/A

          Press ENTER to Confirm or ESC to Cancel:
```

- Select the **'Active'** field to **'Yes'**
- Select the **'Call Direction'** to **'Outgoing'**
- Enter the correct node account for the dial-in router in **'Rem Login'** and **'Rem Password'** fields
- Enter the correct phone number in **'Pri. Phone #'** for dialing to remote router
- Set the **'Bridge'** option to **'Yes'**
- Set the **'Edit IP/IPX/Bridge ='** option to **'Yes'** to turn on the **'Dial-On-Broadcast'** for this outgoing node
- Select the proper **'Transfer Type'** for this connection, in this case it is PPP 64K.
- Enter the idle timer in the **'Idle Timeout'** field for dropping the call if there is no data traffic between the two remote nodes

4. Set the **'Dial-On-Broadcast'** option to **'Yes'** for any broadcasts to trigger the call to the remote node

```
        Menu 11.3 - Remote Node Network Layer Options

IP Options:                    IPX Options:
  Rem IP Addr:                   Dial-On-Query= N/A
  Rem Subnet Mask= N/A           Rem LAN Net #= N/A
  My WAN Addr= N/A               My WAN Net #= N/A
  Single User Account= N/A       Hop Count= N/A
                                 Tick Count= N/A
  Metric= N/A                    W/D Spoofing(min)= N/A
  Private= N/A                   SAP/RIP Timeout(min)= N/A
  RIP Direction= N/A
    Version= N/A             Bridge Options:
                                   Dial-On-Broadcast= Yes
                                   Ethernet Addr Timeout(min)= 0


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

➢ Prestige 2 Setup

1. Enabling the **'Bridge'** option in SMT Menu 1

```
                Menu 1 - General Setup

        System Name= Prestige
        Location= ZyXEL HQ
        Contact Person's Name= abc

        Route IP= No
        Route IPX= No
        Bridge= Yes
```

2. Ethernet Setup in SMT Menu 3

```
            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= 202.113.5.2
          IP Subnet Mask= 255.255.255.0
          RIP Direction= Both
            Version= RIP-2B
```

3. Remote Node Setup in SMT Menu 11

```
Menu 11.1 - Remote Node Profile

  Rem Node Name= P1              Route= None
  Active= Yes                    Bridge= Yes

  Call Direction= Incoming       Edit PPP Options= No
  Incoming:                      Rem IP Addr= N/A
    Rem Login= test              Edit IP/IPX/Bridge= No
    Rem Password= ****           Telco Option:
    Rem CLID=                      Allocated Budget(min)= 0
    Call Back= N/A                 Period(hr)= 0
  Outgoing:                        Transfer Type= 64K
    My Login=                      Nailed-Up Connection= N/A
    My Password=                 Session Options:
    Authen= N/A                    Edit Filter Sets= No
    Pri Phone #= N/A               Idle Timeout(sec)= 100
    Sec Phone #= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

* Select the **'Active'** field to **'Yes'**
* Select the **'Call Direction'** to **'Incoming'**
* Enter the correct node account for the dial-in router in **'Rem Login'** and **'Rem Password'** fields
* Set the **'Bridge'** option to **'Yes'**
* Select the proper **'Transfer Type'** for this connection, in this case it is PPP 64K.

➢ Special handling for certain IPX packets to reduce the number of calls

Bridging is used to forward packets of unsupported protocols whose destination is not on the local Ethernet to the remote LAN. Basically, all non-local packets are bridged to the remote LAN via WAN, however, the Prestige applies a special handling for certain IPX packets to reduce the number of call, depending on the setting of the **'Handle IPX'** option in **SMT Menu 3.4, 'Bridge Ethernet Setup'**.

Menu 3.4 - Bridge Ethernet Setup

Handle IPX= **Client**

✓ None……..Set to 'None' if there is no IPX traffic on the LAN or if you do not want to apply any special handling for IPX.
✓ Client…..…Set to 'Client' if there are only Novell clients on the LAN
✓ Server……Set to 'Server' if there are only Novell servers on the LAN

If there are both Novell clients and servers on the LAN, and the client also want to access the remote Novell server, set to 'Client' and set the 'Dial-On-Broadcast' to on in menu 11.3 to 'Yes' to allow the client queries to trigger the call.

➢ The way Prestige handles certain IPX packets during bridging

✓ **None**
Prestige will do nothing to the IPX traffic

✓ **Client**
All RIP and SAP periodical response packets will not trigger the call

✓ **Server**
No RIP or SAP packets will trigger the call. Besides, during the time when the ISDN line is idle, Prestige will reply to the server's watchdog messages on behalf of remote clients. The period of time that Prestige will do this is linked to the Ethernet Address Timeout parameter in each Remote Node. When a remote Ethernet address is aged out, there is no need to maintain its connection to the IPX server.

IPX Connection

Telecommuter Connection

LAN-to-LAN With One Novell Server

LAN-to-LAN With Two Novell Server

LAN-to-LAN via Prestige and Cisco Routers

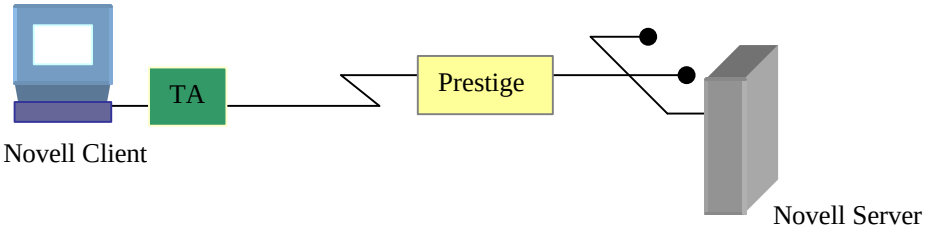
IPX Configuration

Workstation using an ISDN TA to route IPX

➢ Introduction

This configuration note explains how to set up a workstation using an ISDN TA to connect to the Prestige router to route IPX. In this configuration, the workstation has Novell client software so that you will be able to log into the Novell server. There will be two items that you need to set up. These are the workstation and the Prestige router.

➢ Configuration



➢ Setting up the Novell client

To setup the Novell client, you need to set the following parameters

- ❖ Server Name – In some cases, you may need the name that has been configured for the Novell server you wish to login to.

The procedure for configuring these parameters for your workstation may differ depending on the type of IPX client software you are using on your workstation.

➢ Setting up the Prestige

Before configuring the two remote nodes for this application, you need to complete the following settings first in each Prestige router.

- ✓ *General Setup in SMT Menu 1*-entering the system information and turn **'IPX'** on
- ✓ *ISDN Setup in SMT Menu 2- e*ntering your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-entering the IP address of the Prestige and enable the DHCP server if it is required.
- ✓ *Novell IPX Ethernet Setup in SMT menu 3.3*- selecting the correct **'Frame Type'** that your Novell server is running. It is possible to set more than one type.
- ✓ *Default Dial-in Setup in SMT Menu 13*
- ✓ *Edit Dial-in User in SMT Menu 14*

1. Enabling the 'IPX' option in SMT Menu 1

```
                Menu 1 - General Setup

        System Name= Prestige
        Location= ZyXEL US
        Contact Person's Name= abc

        Route IP= No
        Route IPX= Yes
        Bridge= No
```

2. Ethernet Setup in SMT Menu 3

```
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= 202.113.5.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

3. Novell IPX Ethernet Setup

```
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

      Press ENTER to Confirm or ESC to Cancel:
```

* Set **'Seed Router'** to **'No'** since there is a Novell server on your LAN providing the network number
* Select the proper **'Frame Type'** that your Novell server is running

4. Default Dial-in Setup

```
                Menu 13 - Default Dial-in Setup

Telco Options:                    IP Address Supplied By:
  CLID Authen= None                 Dial-in User= Yes
                                    IP Pool= No
PPP Options:                          IP Start Addr= N/A
  Recv Authen= CHAP/PAP               IP Count(1,2)= N/A
  Compression= Yes
  Mutual Authen= No               IPX Net Num Supplied By:
    PAP Login= N/A                  IPX Pool= Yes
    PAP Password= N/A                 IPX Start Net Num= 12345678
  Multiple Link Options:              IPX Count(2,16)= 2
    Max Trans Rate(Kbps)= 128
                                  Session Options:
Callback Budget Management:           Edit Filter Sets= No
  Allocated Budget(min)=              Idle Timeout= 300
  Period(hr)=

          Press ENTER to Confirm or ESC to Cancel:
```

* Set the **'Rev Authen'**. field to the type of authentication you want to use (CHAP, PAP or None).
* Set the **'IPX Pool'** to **'Yes'** to assign the IPX network number to assign a specific network number to remote client
* Set the network number you want to assign to the remote client in the **'IPX Start Net Num. ='** field
* Give the size of the IPX pool in the **'IPX Count'** field, the size can be from 2 to 16 numbers.

5 Edit Dial-in User Setup

```
          Menu 14.1 - Edit Dial-in User

            User Name= test
            Active= Yes
            Password=1234
            Callback= No
              Phone # Supplied by Caller= N/A
              Callback Phone #= N/A
            Rem CLID=
            Idle Timeout= 300
```

* Set the username and password that the client will provide when dialing to the Prestige router
* Set the **'Active'** field to **'Yes'.**

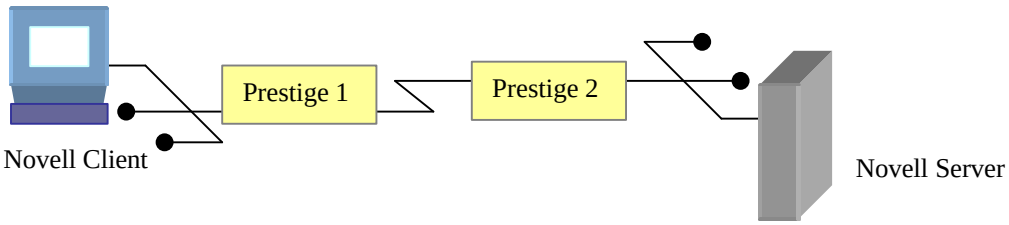
IPX Configuration

LAN-to-LAN connection routing IPX with one Novell server

➢ Introduction

This configuration note explains how to set up a workstation on a network to use a Prestige router to connect to the remote Prestige router to route IPX. In this configuration, the workstation has Novell client software so that you will be able to log into the Novell server. There will be three items that you need to set up. These are the workstation and the two Prestige routers.

➢ Configuration



➢ Setting up the Novell client

To setup the Novell client, you need to set the following parameters

- ❖ Server Name – In some cases, you may need the name that has been configured for the Novell server you wish to login to.

The procedure for configuring these parameters for your workstation may differ depending on the type of IPX client software you are using on your workstation.

➢ Setting up Prestige 1

Before configuring the two remote nodes for this application, you need to complete the following settings first in each Prestige router.

- ✓ *General Setup in SMT Menu 1*-entering the system information and turn **'IPX'** on
- ✓ *ISDN Setup in SMT Menu 2- e*ntering your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-entering the IP address of the Prestige and enable the DHCP server if it is required.
- ✓ *Novell IPX Ethernet Setup in SMT menu 3.3*- selecting the correct **'Frame Type'** that your Novell server is running. It is possible to set more than one type.
  Remote Node Setup in SMT Menu 11

1. Enabling the 'IPX' option in SMT Menu 1

```
                Menu 1 - General Setup

        System Name= Prestige
        Location= ZyXEL HQ
        Contact Person's Name= abc

        Route IP= No
        Route IPX= Yes
        Bridge= No
```

2. Ethernet Setup in SMT Menu 3

```
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= 202.113.5.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

3. Novell IPX Ethernet Setup

```
Menu 3.3 - Novell IPX Ethernet Setup

Seed Router= Yes
Frame Type 802.2= Yes
  IPX Network #= 00002222

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

Press ENTER to Confirm or ESC to Cancel:
```

* Set **'Seed Router'** to **'Yes'** since there is no Novell server on your LAN providing the network number
* Select the proper **'Frame Type'** that your Novell server is running
* Set the **'IPX Network #'** to any valid unique one that is not being used on the network

4. Remote Node Setup

```
                Menu 11.1 - Remote Node Profile

Rem Node Name= P2              Route= IPX
Active= Yes                    Bridge= No

Call Direction= Outgoing       Edit PPP Options= No
Incoming:                      Rem IP Addr= N/A
  Rem Login= N/A               Edit IP/IPX/Bridge= Yes
  Rem Password= N/A            Telco Option:
  Rem CLID= N/A                  Allocated Budget(min)= 0
  Call Back= N/A                 Period(hr)= 0
Outgoing:                        Transfer Type= 64K
  My Login= test                 Nailed-Up Connection= No
  My Password= 1234            Session Options:
  Authen= CHAP/PAP               Edit Filter Sets= No
  Pri Phone #= 5009097           Idle Timeout(sec)= 100
  Sec Phone #=

          Press ENTER to Confirm or ESC to Cancel:
```

- Set the **'Call Direction'** to **'Outgoing'**
- Set the **'Active'** to **'Yes'**
- Set correct username and password that will be used to log into the remote router
- Set the correct phone number of the remote router in **'Pri. Phone'** field
- Set the **'Route'** to **'IPX'**
- Set the **'Edit IP/IPX/Bridge'** to **'Yes'** to set the **'Dial-On-Query'** to **'Yes'**

5. Edit the Menu 11.3

```
        Menu 11.3 - Remote Node Network Layer Options

IP Options:                    IPX Options:
  Rem IP Addr:                   Dial-On-Query= Yes
  Rem Subnet Mask= N/A           Rem LAN Net #= 00000100
  My WAN Addr= N/A               My WAN Net #= 00000000
  Single User Account= N/A       Hop Count= 1
                                 Tick Count= 2
  Metric= N/A                    W/D Spoofing(min)= 3
  Private= N/A                   SAP/RIP Timeout(min)= 3
  RIP Direction= N/A
    Version= N/A               Bridge Options:
                                   Dial-On-Broadcast= N/A
                                   Ethernet Addr Timeout(min)= N/A
```

- Set the **'Dial-On-Query'** to **'Yes'**, this field is necessary for the Prestige on the client side LAN. When set to **'Yes'**, any Get Service SAP or RIP broadcasts coming from the LAN will trigger the call to the remote node.
- Enter the internal network number of the remote Novell server in **'Rem LAN Net # '** field. This number can be obtained by the network administrator.

❖ Enter the WAN network number of the remote device, this number will be used for negotiating between the Prestige and the remote device. If you leave it **'00000000'**, the Prestige will select the greater WAN network number between the two devices.

➢ Setting up Prestige 2

Before configuring the two remote nodes for this application, you need to complete the following settings first in each Prestige router.

- ✓ *General Setup in SMT Menu 1*-entering the system information and turn **'IPX'** on
- ✓ *ISDN Setup in SMT Menu 2- e*ntering your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-entering the IP address of the Prestige and enable the DHCP server if it is required.
- ✓ *Novell IPX Ethernet Setup in SMT menu 3.3*- selecting the correct **'Frame Type'** that your Novell server is running. It is possible to set more than one type.
  Remote Node Setup in SMT Menu 11

1. Enabling the **'IPX'** option in SMT Menu 1

```
Menu 1 - General Setup

System Name= Prestige
Location= ZyXEL US
Contact Person's Name= abc

Route IP= No
Route IPX= Yes
Bridge= No
```

2. Ethernet Setup in SMT Menu 3

```
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= 202.113.10.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

3. Novell IPX Ethernet Setup

```
            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

            Press ENTER to Confirm or ESC to Cancel:
```

* Set **'Seed Router'** to **'No'** since there is a Novell server on your LAN providing the network number
* Select the proper **'Frame Type'** that your Novell server is running

4. Remote Node Setup

```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= P2              Route= IPX
  Active= Yes                    Bridge= No

  Call Direction= Incoming       Edit PPP Options= No
  Incoming:                      Rem IP Addr= N/A
    Rem Login= test              Edit IP/IPX/Bridge= No
    Rem Password= ****           Telco Option:
    Rem CLID=                      Allocated Budget(min)= 0
    Call Back=                     Period(hr)= 0
  Outgoing:                        Transfer Type= 64K
    My Login= N/A                  Nailed-Up Connection= No
    My Password= N/A             Session Options:
    Authen= N/A                      Edit Filter Sets= No
    Pri Phone #= N/A                 Idle Timeout(sec)= 100
    Sec Phone #=N/A

              Press ENTER to Confirm or ESC to Cancel:
```

- Set the **'Call Direction'** to **'Incoming'**
- Set the **'Active'** to **'Yes'**
- Set a username and password for the remote router to log in
- Set the **'Route'** to **'IPX'**

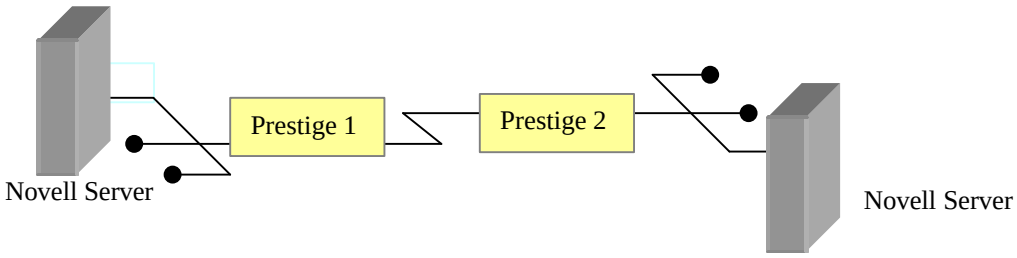
IPX Configuration

LAN-to-LAN connection routing IPX with two Novell servers

➢ Introduction

This configuration note explains how to set up a workstation on a network to use a Prestige router to make a connection to another Prestige router to route IPX. In this configuration, the workstation has Novell client software so that you will be able to log into the Novell server. There will be three items that you need to set up. These are the workstation and the two Prestige routers.

➢ Configuration



➢ Setting up the Novell client

To setup the Novell client, you need to set the following parameters

- ❖ Server Name – In some cases, you may need the name that has been configured for the Novell server you wish to login to.

The procedure for configuring these parameters for your workstation may differ depending on the type of IPX client software you are using on your workstation.

➢ Setting up the Prestige 1

Before configuring the two remote nodes for this application, you need to complete the following settings first in each Prestige router.

- ✓ *General Setup in SMT Menu 1*-entering the system information and turn **'IPX'** on
- ✓ *ISDN Setup in SMT Menu 2- e*ntering your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-entering the IP address of the Prestige and enable the DHCP server if it is required.
- ✓ *Novell IPX Ethernet Setup in SMT menu 3.3*- selecting the correct **'Frame Type'** that your Novell server is running. It is possible to set more than one type
- ✓ *Remote Node Setup in SMT Menu 11*

1. Enabling the **'IPX'** option in SMT Menu 1

```
                Menu 1 - General Setup

        System Name= Prestige
        Location= ZyXEL HQ
        Contact Person's Name= abc

        Route IP= No
        Route IPX= Yes
        Bridge= No
```

2. Ethernet Setup in SMT Menu 3

```
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= 202.113.5.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

3. Novell IPX Ethernet Setup

```
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

Press ENTER to Confirm or ESC to Cancel:
```

* Set **'Seed Router'** to **'No'** since there is a Novell server on your LAN providing the network number
* Select the proper **'Frame Type'** that your Novell server is running

4. Remote Node Setup

```
                Menu 11.1 - Remote Node Profile

Rem Node Name= P2              Route= IPX
Active= Yes                    Bridge= No

Call Direction= Outgoing       Edit PPP Options= No
Incoming:                      Rem IP Addr= N/A
  Rem Login= N/A               Edit IP/IPX/Bridge= Yes
  Rem Password= N/A            Telco Option:
  Rem CLID= N/A                  Allocated Budget(min)= 0
  Call Back= N/A                 Period(hr)= 0
Outgoing:                        Transfer Type= 64K
  My Login= test                 Nailed-Up Connection= No
  My Password= 1234            Session Options:
  Authen= CHAP/PAP               Edit Filter Sets= No
  Pri Phone #= 5009097           Idle Timeout(sec)= 100
  Sec Phone #=

          Press ENTER to Confirm or ESC to Cancel:
```

- Set the **'Call Direction'** to **'Outgoing'**
- Set the **'Active'** to **'Yes'**
- Set correct username and password that will be used to log into the remote router
- Set the correct phone number of the remote router in **'Pri. Phone'** field
- Set the **'Route'** to **'IPX'**
- Set the **'Edit IP/IPX/Bridge'** to **'Yes'** to set the **'Dial-On-Query'** to **'Yes'**

5. Edit the Menu 11.3

```
          Menu 11.3 - Remote Node Network Layer Options

IP Options:                    IPX Options:
  Rem IP Addr:                   Dial-On-Query= Yes
  Rem Subnet Mask= N/A           Rem LAN Net #= 00000100
  My WAN Addr= N/A               My WAN Net #= 00000000
  Single User Account= N/A       Hop Count= 1
                                 Tick Count= 2
  Metric= N/A                    W/D Spoofing(min)= 3
  Private= N/A                   SAP/RIP Timeout(min)= 3
  RIP Direction= N/A
    Version= N/A               Bridge Options:
                                   Dial-On-Broadcast= N/A
                                   Ethernet Addr Timeout(min)= N/A
```

- Set the **'Dial-On-Query'** to **'Yes'**, this field is necessary for the Prestige on the client side LAN. When set to **'Yes'**, any Get Service SAP or RIP broadcasts coming from the LAN will trigger the call to the remote node.
- Enter the internal network number of the remote Novell server in **'Rem LAN Net # '** field. This number can be obtained from the network administrator.

❖ Enter the WAN network number of the remote device, this number will be used for negotiating between Prestige and remote device. If you leave it '00000000', the Prestige will select the greater WAN network number between the two devices.

➢ Setting up the Prestige 2

Before configuring the two remote nodes for this application, you need to complete the following settings first in each Prestige router.

- ✓ *General Setup in SMT Menu 1*-entering the system information and turn **'IPX'** on
- ✓ *ISDN Setup in SMT Menu 2- e*ntering your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-entering the IP address of the Prestige and enable the DHCP server if it is required.
- ✓ *Novell IPX Ethernet Setup in SMT menu 3.3*- selecting the correct **'Frame Type'** that your Novell server is running. It is possible to set more than one type.
  Remote Node Setup in SMT Menu 11

1. Enabling the **'IPX'** option in SMT Menu 1

```
                Menu 1 - General Setup

        System Name= Prestige
        Location= ZyXEL US
        Contact Person's Name= abc

        Route IP= No
        Route IPX= Yes
        Bridge= No
```

2. Ethernet Setup in SMT Menu 3

```
            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= 202.113.10.1
          IP Subnet Mask= 255.255.255.0
          RIP Direction= Both
            Version= RIP-2B
```

3. Novell IPX Ethernet Setup

```
        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

        Press ENTER to Confirm or ESC to Cancel:
```

* Set **'Seed Router'** to **'No'** since there is a Novell server on your LAN providing the network number
* Select the proper **'Frame Type'** that your Novell server is running

4. Remote Node Setup

```
                Menu 11.1 - Remote Node Profile

Rem Node Name= P2              Route= IPX
Active= Yes                    Bridge= No

Call Direction= Incoming       Edit PPP Options= No
Incoming:                      Rem IP Addr= N/A
  Rem Login= test              Edit IP/IPX/Bridge= No
  Rem Password= 1234            Telco Option:
  Rem CLID= N/A                   Allocated Budget(min)= 0
  Call Back= N/A                  Period(hr)= 0
Outgoing:                         Transfer Type= 64K
  My Login= N/A                   Nailed-Up Connection= No
  My Password= N/A             Session Options:
  Authen= CHAP/PAP                Edit Filter Sets= No
  Pri Phone #=                    Idle Timeout(sec)= 100
  Sec Phone #=

        Press ENTER to Confirm or ESC to Cancel:
```

- Set the **'Call Direction'** to **'Incoming'**
- Set the **'Active'** to **'Yes'**
- Set a username and password for the remote router to log in
- Set the **'Route'** to **'IPX'**

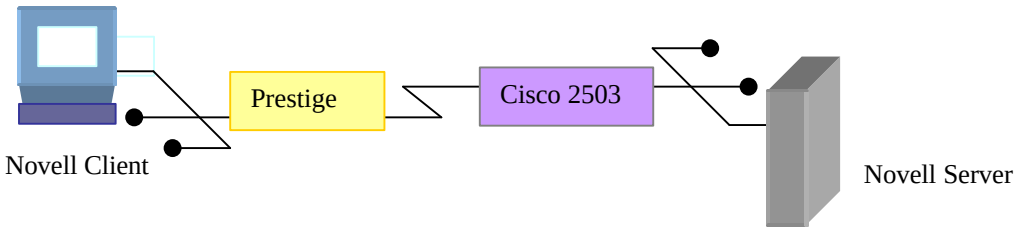
IPX Configuration

LAN-to-LAN connection routing IPX with Novell client on Prestige side and Novell server on Cisco side

➢ Introduction

This configuration note explains how to set up a workstation on a network to use a Cisco 2503 to make a connection to a Prestige router to route IPX. In this configuration, the workstation has Novell client software so that you will be able to log into the Novell server. There will be three items that you need to set up. These are the workstation, Cisco 2503 and Prestige router.

➢ Configuration



➢ Setting up the Novell client

To setup the Novell client, you need to set the following parameters

- ❖ Server Name – In some cases, you may need the name that has been configured for the Novell server you wish to login to.

The procedure for configuring these parameters for your workstation may differ depending on the type of IPX client software you are using on your workstation.

➢ Setting up Prestige Router

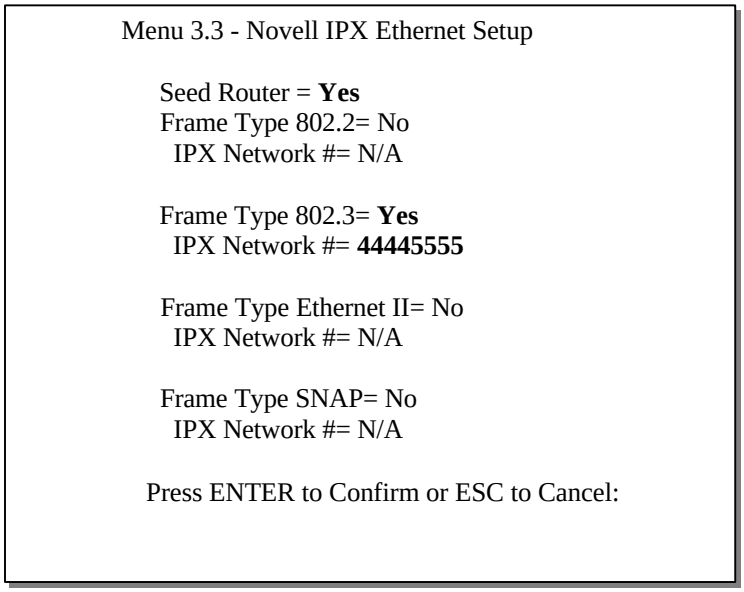
Before configuring the two remote nodes for this application, you need to complete the following settings first in each Prestige router.

- ✓ *General Setup in SMT Menu 1*-entering the system information and turn **'IPX'** on
- ✓ *ISDN Setup in SMT Menu 2- e*ntering your ISDN number
- ✓ *Ethernet Setup in SMT Menu 3*-entering the IP address of the Prestige and enable the DHCP server if it is required.
- ✓ *Novell IPX Ethernet Setup in SMT menu 3.3*- selecting the correct 'Frame Type' that your Novell server is running. It is possible to set more than one type.
- ✓ *Remote Node Setup in SMT Menu 11*

1. Enabling the 'IPX' option in SMT Menu 1

```
                Menu 1 - General Setup

        System Name= Prestige
        Location= ZyXEL HQ
        Contact Person's Name= abc

        Route IP= Yes
        Route IPX= Yes
        Bridge= No
```

2. Novell IPX Ethernet Setup



Menu 3.3 - Novell IPX Ethernet Setup

Seed Router = **Yes**
Frame Type 802.2= No
IPX Network #= N/A

Frame Type 802.3= **Yes**
IPX Network #= **44445555**

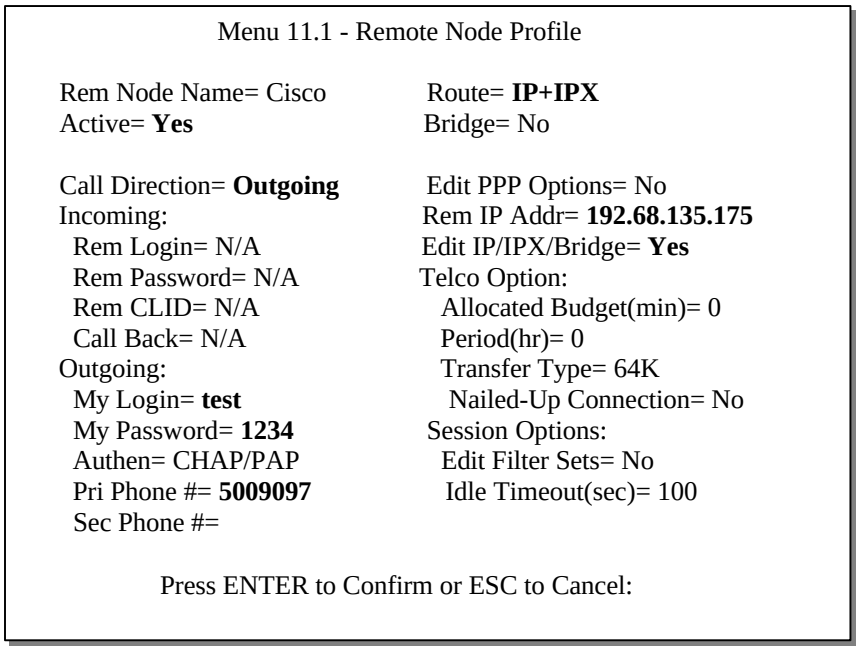
Frame Type Ethernet II= No
IPX Network #= N/A

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

Press ENTER to Confirm or ESC to Cancel:

* Set **'Seed Router'** to **'Yes'** since there is no Novell server on your LAN providing the network number
* Select the proper **'Frame Type'** that your Novell server is running
* Set the **'IPX Network #'** to any valid unique one that is not being used on the network.

3. Remote Node Setup



Menu 11.1 - Remote Node Profile

Rem Node Name= Cisco
Active= **Yes**

Call Direction= **Outgoing**
Incoming:
Rem Login= N/A
Rem Password= N/A
Rem CLID= N/A
Call Back= N/A
Outgoing:
My Login= **test**
My Password= **1234**
Authen= CHAP/PAP
Pri Phone #= **5009097**
Sec Phone #=

Route= **IP+IPX**
Bridge= No

Edit PPP Options= No
Rem IP Addr= **192.68.135.175**
Edit IP/IPX/Bridge= **Yes**
Telco Option:
Allocated Budget(min)= 0
Period(hr)= 0
Transfer Type= 64K
Nailed-Up Connection= No
Session Options:
Edit Filter Sets= No
Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

- Set the **'Call Direction'** to **'Outgoing'**
- Set the **'Active'** to **'Yes'**
- Set correct username and password that will be used to log into the remote router
- Set the correct phone number of the remote router in **'Pri. Phone'** field
- Set the **'Route'** to **'IP+IPX'**

- Enter the correct IP address of the remote Cisco router in **'Rem IP Addr'** field
- Set the **'Edit IP/IPX/Bridge'** to **'Yes'** to set the **'Dial-On-Query'** to **'Yes'**

4. Edit the Menu 11.3

```
        Menu 11.3 - Remote Node Network Layer Options

IP Options:                    IPX Options:
  Rem IP Addr:192.68.135.175     Dial-On-Query= Yes
  Rem Subnet Mask= 0.0.0.0       Rem LAN Net #= 00001111
  My WAN Addr= 0.0.0.0           My WAN Net #= 00000000
  Single User Account= N/A       Hop Count= 1
                                 Tick Count= 2
  Metric= N/A                    W/D Spoofing(min)= 3
  Private= N/A                   SAP/RIP Timeout(min)= 3
  RIP Direction= N/A
    Version= N/A               Bridge Options:
                                   Dial-On-Broadcast= N/A
                                   Ethernet Addr Timeout(min)= N/A
```

- Set the **'Dial-On-Query'** to **'Yes'**, this field is necessary for the Prestige on the client side LAN. When set to **'Yes'**, any Get Service SAP or RIP broadcasts coming from the LAN will trigger the call to the remote node.
- Enter the internal network number of the remote Novell server in **'Rem LAN Net # '** field. This number can be obtained from the network administrator.
- Enter the WAN network number of the remote device, this number will be used for negotiating between Prestige and remote device. If you leave it '00000000', the Prestige will select the greater WAN network number between the two devices.

➢ Setting up Cisco router

Following is a capture of **'wr t'** command. Please note those fields are indicated in bold type.

```
#####
Current configuration:
!
version 10.2
service password-encryption
!
hostname csco2503
!
enable password 7 03085A09
!
username Prestige password 7 00554155500E
ip subnet-zero
no ip domain-lookup
ipx routing
isdn switch-type basic-dms100
!
interface Ethernet0
```

```
ip address 192.68.135.175 255.255.255.0
ipx network 00003333
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
ip unnumbered Ethernet0
encapsulation ppp
ipx network 44445555
dialer idle-timeout 300
dialer map ip 204.247.203.176 name Prestige 5551212
dialer map ipx 44445555.00a0.c510.0074 name Prestige broadcast
!               **** 00a0:c510:0074 is the Mac address in Prestige
dialer-group 1
ppp authentication pap
!
ip classless
ip route 204.247.203.0 255.255.255.0 BRI0
ip route 204.247.203.156 255.255.255.255 BRI0
no logging console
!
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol novell permit
!
      :
      :
!
end
```

Filter Examples

How does ZyXEL Filter work?

Conceptually, there are two categories of filter rules: ***device*** and ***protocol***. The Generic filter rules belong to the *device* category; they act on the raw data from/to LAN and WAN. The IP and IPX filter rules belong to *protocol* category; they act on the IP and IPX packets.

In order to allowing users to specify the local network IP address and port number in the filter rules with SUA connections, the TCP/IP filter function has to be executed **before** SUA for WAN outgoing packets and **after** the SUA for WAN incoming IP packets. But at the same time, the Generic filter rules must be applied at the point when Prestige is receiving and sending the packets; i.e. the ISDN interface. So, the execution sequence has to be changed. The logic flow of the filter is shown in **Figure 1** and the sequence of the logic flow for the packet from LAN to WAN is:

1. LAN device and protocol input filter sets.
2. WAN protocol call and output filter sets. It works now because SUA does not convert the local IP address and port number to WAN IP address and port number yet.
3. SUA converts the source IP address from 192.168.1.33 to 203.205.115.6 and port number from 1023 to 4034.
4. WAN device output and call filter sets.

The sequence of the logic flow for the packet from WAN to LAN is:

5. WAN device input filter sets.
6. SUA converts the destination IP address from 203.205.115.6 to 192.168.1.33 and port number from 4034 to 1023.
7. WAN protocol input filter sets. It works now because SUA has converted the destination IP address and port number to local IP address and port number.
8. LAN device and protocol output filter sets.

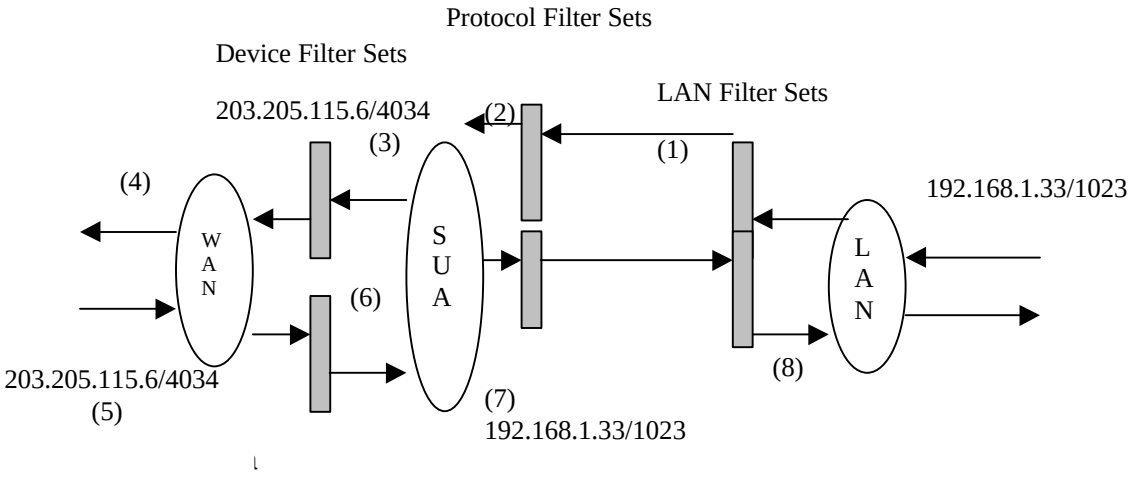


Figure 1. Packet Logic Flow in ZyNOS

Generic and **TCP/IP (and IPX)** filter rules must now be in different filter sets. The SMT will detect and prevent the mixing of different category rules within any filter set in Menu 21. In the following example, you will receive an error message **"Protocol and device filter rules cannot be active**

together" if you try to activate a TCP/IP (or IPX) filter rule in a filter set that has already had one or more active Generic filter rules. You will receive the same error if you try to activate a Generic filter rule in a filter set that has already had one or more active TCP/IP (or IPX) filter rules.

Menu 21.1.1:

```
                Menu 21.1.1 - Generic Filter Rule

            Filter #: 1,1
            Filter Type= Generic Filter Rule
            Active= Yes
            Offset= 0
            Length= 0
            Mask= N/A
            Value= N/A
            More= No                        Log= None
            Action Matched= Check Next Rule
            Action Not Matched= Check Next Rule
```

Menu 21.1.2:

```
                Menu 21.1.2 - TCP/IP Filter Rule

            Filter #: 1,2
            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= 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= Check Next Rule
            Action Not Matched= Check Next Rule

            Press ENTER to Confirm or ESC to Cancel:
Saving to ROM.  Please wait...
Protocol and device rule cannot be active together
```

To separate the device and protocol filter categories; two new menus, Menu 11.5 and Menu 13.1, have been added, as well as some changes made to the Menu 3.1, Menu 11.1, and Menu 13. The changed fields are marked **black** in the following menus:

Menu 3.1:

```
                Menu 3.1 - General Ethernet Setup

              Ethernet Interface= 10BaseT
              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=
```

Menu 11.1:

```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= abc
  Active= Yes                       Route= IP
  Call Direction= Outgoing          Bridge= No
  Tunneling Mode= None
    Endpoint Index= N/A             Edit PPP Options= No
                                    Rem IP Addr= 0.0.0.0
  Incoming:                         Edit IP/IPX/Bridge= No
    Rem Login= N/A                  Telco Option:
    Rem Password= N/A                 Allocated Budget(min)= 0
    Rem CLID= N/A                     Period(hr)= 0
    Call Back= N/A                  Transfer Type= 64K
  Outgoing:                         Nailed-Up Connection= No
    My Login= xyxw                  Session Options:
    My Password= ********             Edit Filter Sets= Yes
    Authen= CHAP/PAP                  Idle Timeout(sec)= 300
    Pri Phone #= 140812345678
    Sec Phone #= 140822345678
            Press ENTER to Confirm or ESC to Cancel:
```

Menu 11.5:

```
            Menu 11.5 - Remote Node Filter

        Input Filter Sets:
          protocol filters=
            device filters=
        Output Filter Sets:
          protocol filters=
            device filters=
        Call Filter Sets:
          protocol filters=
            device filters=
```

Menu 13:

```
                    Menu 13 - Default Dial-in Setup

Telco Options:                      IP Address Supplied By:
  CLID Authen= None                   Dial-in User= Yes
                                      IP Pool= Yes
PPP Options:                            IP Start Addr= 123.234.111.163
  Recv Authen= CHAP/PAP                 IP Count(1,2)= 2
  Compression= Yes
  Mutual Authen= No                 IPX Net Num Supplied By:
    PAP Login= N/A                    IPX Pool= Yes
    PAP Password= N/A                   IPX Start Net Num= a0000001
  Multiple Link Options:                IPX Count(2,16)= 2
    Max Trans Rate(Kbps)= 128
                                    Session Options:
Callback Budget Management:           Edit Filter Sets= Yes
  Allocated Budget(min)=              Idle Timeout= 300
  Period(hr)=
```

Menu 13.1:

```
            Menu 13.1 - Default Dial-in Filter

        Input Filter Sets:
          protocol filters=
            device filters=
        Output Filter Sets:
          protocol filters=
            device filters=
```

SMT will also prevent you entering a protocol filter set configured in Menu 21 to the ***device filters*** field in Menu 3.1, 11.5, or 13.1, or entering a device filter set to the ***protocol filters*** field. Even though SMT will prevent the inconsistency from being entered in ZyNOS, it is unable to resolve the intermixing problems existing in the filter sets that were configured before. Instead, when ZyNOS

translates the old configuration into the new format, it will verify the filter rules and log the inconsistencies. Please check the system log (Menu 24.3.1) before putting your device into production.

Running the Prestige with wrong filter rules may cause it to keep the ISDN line perpetually active, and/or allow undesired traffic to pass to the outside world, and receive unwanted outside traffic. The first case may incur an enormous ISDN bill; the second may be a data security hazard.

In order to avoid operational problems later, the Prestige will disable its routing/bridging functions if there is an inconsistency among its filter rules.

How do I know what LAN packet triggers the call?

If the user already knows the protocol type, the source port and the IP address of the packet that triggering the call, he can design the filter rule based on these information. Otherwise, he can take a look at the SMT Menu 24.1 to see what is the exact packet that triggers the outgoing call. The 'LAN Packet Which Triggered Last Call' status in Menu 24.1 will show you the packet which triggers the call. This is a display of the header of the packets as below:

LAN Packet which Triggered Last Call: (Type: IP)
45 00 00 2E CA 0E 40 00 1F 06 D7 09 CC F7 CB B4 CC D9 00 02 04 1C 00 15
00 33 2D 5E 55 80 B5 C0 50 18 1F 9B E7 D4 00 00 50 41 53 56 0D 0A

To know more about the format of the IP packet and IPX packet in Menu 24.1 for you to configure a filter rule, we list the header of the IP, UDP and TCP as following. Some examples of the packets will show you after the headers.

IP Header

0 15 16 31

4-bit version	4-bit length	8-byte type of service (TOS)	16-bit total length (in bytes)
16-bit identification		3-bit flag	13-bit fragment offset
8-bit time to live(TTL)	8-bit protocol	16-bit header checksum	
32-bit source IP address			
32-bit destination IP address			
Option (if any)			
Data			

UDP Header

0 15 16 31

16-bit source port number	16-bit destination port number
16-bit UDP length	16-bit UDP checksum
Data (if any)	

TCP Header

0 15 16 31

16-bit source port number								16-bit destination port number
32-bit sequence number								
32-bit acknowledgment number								
4-bit header length	Reserved(6 bits)	**URG**	**ACK**	**PSH**	**RST**	**SYN**	**FIN**	16-bit window size
16-bit TCP checksum								16-bit urgent pointer
Option (if any)								
Data (if any)								

Based on the above headers, we then can interpret the LAN Packet Which Triggered Last Call to as following:

LAN Packet which Triggered Last Call : (Type: IP)
45 00 00 2E CA 0E 40 00 1F **06** D7 09 **CC F7 CB B4** **CC D9 00 02** **04 1C** **00 15**

Protocol = 6 = TCP
Source IP = 204.247.203.180 (source IP)
Destination IP = 204.217.0.2 (destination IP)
Source port number = 1052 (41Ch)
Destination port number = 21 (15h) = ftp

IPX header in Menu 24.1:

LAN Packet Which Triggered Last Call: (Type: IPX)
00 28 01 **01** **00 00 00 00** **FF FF FF FF FF FF** **04 53** **00 00 00 00** **00 00 00 00 00 00** **04 53** 00 01
FF FF FF FF FF 00 00 00 00

IPX packet type
Destination network number
Destination node number
Destination socket number
Source network number
Source node number
Source socket number

IPX packet type:
01=RIP
02=echo
03=error
04=SAP
05=SPX
11=NCP
14=NetBIOS

Socket number:
0451=NCP
0451=SAP
0453=RIP
0455=NetBIOS

Filter

How do I forbid the web request from the workstation triggering a call?

➢ Introduction

If you want to avoid the outbound Web request to trigger a call to remote, you can configure a call filter set in Prestige to block this packet. After the call filter is applied, the Web packet will not trigger the call to your ISP or remote node. However, when the call is trigger by the other packets and the Internet connection is established, the workstations then are able to access the Web page.

➢ Configuration

Before configuring a filter, you need to know the following information:

1. The outbound packet type (protocol & port number)
2. The source IP address

Generally, the outbound packets for Web service could be as following:

a. HTTP packet, TCP (06) protocol with port number 80
b. DNS packet, TCP (06) protocol with port number 53 or
c. DNS packet, UDP (17) protocol with port number 53

For all workstation on the LAN, the source IP address will be 0.0.0.0. Otherwise, you have to enter an IP Address for the workstation you want to block. See the procedure for configuring this filter below.

✓ Create a filter set in Menu 21, e.g., set 1
✓ Create three filter rules in Menu 21.1.1, Menu 21.1.2, Menu 21.1.3

❖ *Rule 1*- block the HTTP packet, TCP (06) protocol with port number 80
❖ *Rule 2*- block the DNS packet, TCP (06) protocol with port number 53
❖ *Rule 3*- block the DNS packet, UDP (17) protocol with port number 53

✓ Apply the filter set in remote node, Menu 11

✓ Create a filter set in Menu 21

```
                Menu 21 – Filter Set Configuration

Filter                                  Filter
Set #       Comments                    Set #       Comments
------  -----------------               ------  -----------------
  1     Web Request                       7     _________________
  2     _________________                 8     _________________
  3     _________________                 9     _________________
  4     _________________                 10    _________________
  5     _________________                 11    _________________
  6     _________________                 12    _________________

            Enter Filter Set Number to Configure= 1
            Edit Comments=
            Press ENTER to Confirm or ESC to Cancel:
```

- Rule one for (a). http packet, TCP(06)/Port number 80

Menu 21.1.1 - TCP/IP Filter Rule

Filter #: 1,1
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 #= **80**
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= **Drop**
Action Not Matched= **Check Next Rule**

Press ENTER to Confirm or ESC to Cancel:

- Rule 2 for (b).DNS request, TCP(06)/Port number 53

Menu 21.1.2 - TCP/IP Filter Rule

Filter #: 1,2
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 #= **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= **Drop**
Action Not Matched= **Check Next Rule**

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

❖ Rule 3 for (c). DNS packet UDP(17)/Port number 53

```
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 #= 53
                Port # Comp= Equal
            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= Drop
        Action Not Matched= Forward

    Press ENTER to Confirm or ESC to Cancel:
```

❖ After the three rules are completed, you will see the rule summary in Menu 21.

```
            Menu 21.1 - Filter Rules Summary

# A Type                Filter Rules                M m n
- - ---- ------------------------------------------------------------ -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80    N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=53    N D N
3 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=53   N D F

            Menu 21 - Filter Set Configuration
```

Then put the filter set number '**1**' in the '**Call Filter Set**' field of SMT menu 11.5 for taking active.

```
          Menu 11.1 - Remote Node Profile

        Rem Node Name= hinet          Route= IP
        Active= Yes                   Bridge= No

        Call Direction= Outgoing      Edit PPP Options= No
        Incoming:                     Rem IP Addr= 0.0.0.0
          Rem Login= N/A              Edit IP/IPX/Bridge= No
          Rem Password= N/A           Telco Option:
          Rem CLID= N/A                 Allocated Budget(min)= 0
          Call Back= N/A                Period(hr)= 0
        Outgoing:                       Transfer Type= 64K
          My Login= masterbc            Nailed-Up Connection= No
          My Password= ********       Session Options:
          Authen= CHAP/PAP              Edit Filter Sets= Yes
          Pri Phone #= 4125678          Idle Timeout(sec)= 300
          Sec Phone #=

                Press ENTER to Confirm or ESC to Cancel:
```

Menu 11.5 - Remote Node Filter

Input Filter Sets:
protocol filters=
device filters=
Output Filter Sets:
protocol filters=
device filters=
Call Filter Sets:
protocol filters= **1**
device filters=

Filter

How do I forbid one client triggering the call to Internet?

➢ Introduction

If you want to forbid a specific local client triggering the call to ISP, you can configure a call filter set in Prestige to block the packets from this client. After the call filter is applied, the packet sent from this client will not trigger the call to your ISP or remote node. As long as the call is trigger by the other clients and the Internet connection is established, this workstation is able to access the Internet or remote node.

➢ Configuration

✓ Create a filter set in Menu 21, e.g., set 1

```
                Menu 21 – Filter Set Configuration

Filter                                  Filter
Set #       Comments                    Set #       Comments
------  ----------------                ------  ----------------
  1     Block one client                  7     _________________
  2     _________________                 8     _________________
  3     _________________                 9     _________________
  4     _________________                10     _________________
  5     _________________                11     _________________
  6     _________________                12     _________________

                Enter Filter Set Number to Configure= 1
                Edit Comments=
                Press ENTER to Confirm or ESC to Cancel:
```

❖ One rule one for blocking all packets from this client

```
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= 192.68.135.5
                        IP Mask= 255.255.255.255
                        Port #= 0
                        Port # Comp= None
                TCP Estab= No
                More= No          Log= None
                Action Matched= Drop
                Action Not Matched= Forward

          Press ENTER to Confirm or ESC to Cancel:
```

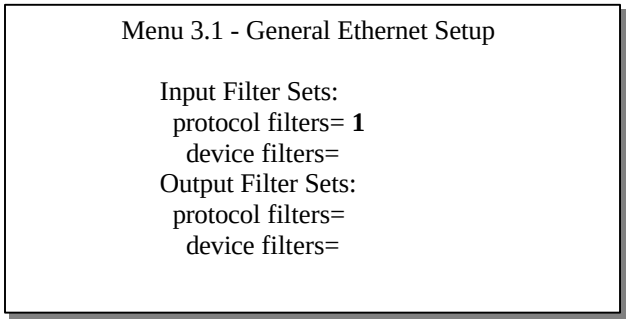
- ✓ *Source IP addr*……Enter the client IP in this field
- ✓ *IP Mask*…….here the IP mask is used to mask the bits of the IP address given in the **‘ Source IP Addr= ‘** field, for one workstation it is **255.255.255.255**.
- ✓ Action Matched…….Set to **‘Drop’** to drop all the packets from this client
- ✓ Action Not Matched……..Set to **‘Forward’** to allow the packets from other clients

Then put the filter set number **'1'** in the **'Call Filter Set'** field of SMT menu 11.5 for taking active.

```
                Menu 11.1 - Remote Node Profile

      Rem Node Name= hinet          Route= IP
      Active= Yes                   Bridge= No

      Call Direction= Outgoing      Edit PPP Options= No
      Incoming:                     Rem IP Addr= 0.0.0.0
        Rem Login= N/A              Edit IP/IPX/Bridge= No
        Rem Password= N/A           Telco Option:
        Rem CLID= N/A                 Allocated Budget(min)= 0
        Call Back= N/A                Period(hr)= 0
      Outgoing:                       Transfer Type= 64K
        My Login= masterbc            Nailed-Up Connection= No
        My Password= ********       Session Options:
        Authen= CHAP/PAP              Edit Filter Sets= Yes
        Pri Phone #= 4125678          Idle Timeout(sec)= 300
        Sec Phone #=

                Press ENTER to Confirm or ESC to Cancel:
```

```
                Menu 11.5 - Remote Node Filter

      Input Filter Sets:
            protocol filters=
            device filters=
      Output Filter Sets:
            protocol filters=
            device filters=
      Call Filter Sets:
            protocol filters= 1
            device filters=
```

- If you want to forbid this client accessing the Internet or remote node, you can apply this filter set to SMT Menu 3.1, the **'protocol filter'** in the Input Filter Sets



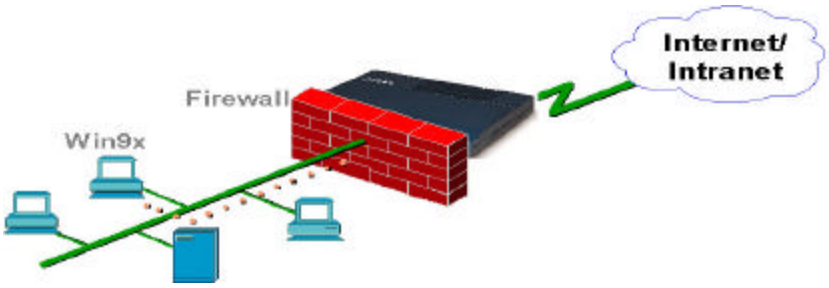
- ✓ After this filter set is applied to this field, the client (192.68.135.5) will not be allowed to access the Internet or remote node any more.

Filter Setup

How do I forbid the NETBIOS packets triggering a call?

- Introduction

The NETBIOS packets contain some port numbers and need to be blocked in this case.
They are port number 137, 138 and 139 with UDP or TCP protocol. In addition, the NETBIOS packet that is used to looking for a remote DNS server via Prestige can also trigger the call. Therefore, the filter rules should cover the above packets.



- Configuration

The packets need to be blocked are as follows. Please configure two filter sets with 4 and 2 rules respectively based on the following packets in SMT menu 21.

Filter Set 1:

- *Rule 1*-Destination port number 137 with protocol number 6 (TCP)
- *Rule 2*-Destination port number 137 with protocol number 17 (UDP)
- *Rule 3*-Destination port number 138 with protocol number 6 (TCP)
- *Rule 4*-Destination port number 138 with protocol number 17 (UDP)
- *Rule 5*-Destination port number 139 with protocol number 6 (TCP)
- *Rule 6*-Destination port number 139 with protocol number 17 (UDP)

Filter Set 2:

- *Rule 1*-Source port number 137, Destination port number 53 with protocol number 6 (TCP)
- *Rule 2*-Source port number 137, Destination port number 53 with protocol number 17 (UDP)

Before starting to set the filter rules, please enter a name for each filter set in the **'Comments'** field first.

```
                    Menu 21 - Filter Set Configuration

 Filter                              Filter
 Set #    Comments                   Set #    Comments
 ------  ----------------            ------  ----------------
   1     NetBIOS#1                     7     _______________
   2     NetBIOS#2                     8     _______________
   3     _______________               9     _______________
   4     _______________              10     _______________
   5     _______________              11     _______________
   6     _______________              12     _______________

                 Enter Filter Set Number to Configure= 1
                 Edit Comments=
                 Press ENTER to Confirm or ESC to Cancel:
```

Configure the first filter set **'NetBIOS#1'** by selecting the Filter Set number **1**.

- *Rule 1*-Destination port number 137 with protocol number 6 (TCP)

```
                Menu 21.1.1 - TCP/IP Filter Rule

                Filter #: 1,1
                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 #= 137
                        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= Drop
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:
```

❖ *Rule 2*-Destination port number 137 with protocol number 17 (UDP)

```
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 #= 137
               Port # Comp= Equal
       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= Drop
  Action Not Matched= Check Next Rule

  Press ENTER to Confirm or ESC to Cancel:
```

❖ *Rule 3*-Destination port number 138 with protocol number 6 (TCP)

```
Menu 21.1.3 - 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 #= 138
               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= Drop
  Action Not Matched= Check Next Rule

  Press ENTER to Confirm or ESC to Cancel:
```

❖ *Rule 4*-Destination port number 138 with protocol number 17 (UDP)

```
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 #= 138
        Port # Comp= Equal
    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= Drop
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
```

❖ *Rule 5*-Destination port number 139 with protocol number 6 (TCP)

```
Menu 21.1.5 - TCP/IP Filter Rule

Filter #: 1,5
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 #= 139
        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= Drop
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
```

❖ *Rule 6*-Destination port number 139 with protocol number 17 (UDP)

```
Menu 21.1.6 - TCP/IP Filter Rule

Filter #: 1,6
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 #= 139
        Port # Comp= Equal
    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= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
```

After the first filter set is finished, you will get the complete rules summary as below.

```
# A Type              Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137          N D N
2 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137         N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138          N D N
4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138         N D N
5 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139          N D N
6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139         N D F
```

Please apply this first filter set **'NetBIOS#1'** to the **'Protocol Filter'** of the **'Call Filter Sets='** in the remote node setup 11.5 for taking active. You can enter to the menu 11.5 by selecting the **'Edit Filter Sets='** in menu 11.1 to **'Yes'.**

Menu 11.1 - Remote Node Profile

Rem Node Name= hinet	Route= IP
Active= Yes	Bridge= No
Call Direction= Outgoing	Edit PPP Options= No
Incoming:	Rem IP Addr= 0.0.0.0
Rem Login= N/A	Edit IP/IPX/Bridge= No
Rem Password= N/A	Telco Option:
Rem CLID= N/A	Allocated Budget(min)= 0
Call Back= N/A	Period(hr)= 0
Outgoing:	Transfer Type= 64K
My Login= masterbc	Nailed-Up Connection= No
My Password= ********	Session Options:
Authen= CHAP/PAP	Edit Filter Sets= **Yes**
Pri Phone #= 4125678	Idle Timeout(sec)= 300
Sec Phone #=	

Press ENTER to Confirm or ESC to Cancel:

Menu 11.5 - Remote Node Filter

Input Filter Sets:
protocol filters=
device filters=
Output Filter Sets:
protocol filters=
device filters=
Call Filter Sets:
protocol filters= **1**
device filters=

Configure the second filter set **'NetBIOS#2'** by selecting the Filter Set number **2**.

- *Rule 1*-Source port number 137, Destination port number 53 with protocol number 6 (TCP)

```
Menu 21.2.1 - TCP/IP Filter Rule

Filter #: 2,1
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 #= 53
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 137
             Port # Comp= Equal
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
```

- *Rule 2*-Source port number 137, Destination port number 53 with protocol number 17 (UDP)

```
Menu 21.2.2 - TCP/IP Filter Rule

Filter #: 2,2
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 #= 53
             Port # Comp= Equal
     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

Press ENTER to Confirm or ESC to Cancel:
```

After the first filter set is finished, you will get the complete rules summary as below.

```
                    Menu 21.2 - Filter Rules Summary

# A Type              Filter Rules                                  M m n
- - ---- ---------------------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                N D N
2 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53               N D F
```

Please apply this second filter set 'NetBIOS#2' in the **'protocol filters='** of the **'Input Filter Sets:'** in the Menu 3 for blocking the packets from LAN interface.

```
            Menu 3.1 - General Ethernet Setup

        Input Filter Sets:
                protocol filters= 2
                device filters=
        Output Filter Sets:
                protocol filters=
                device filters=
```

Filter

How can I set up my Prestige router as an Internet firewall?

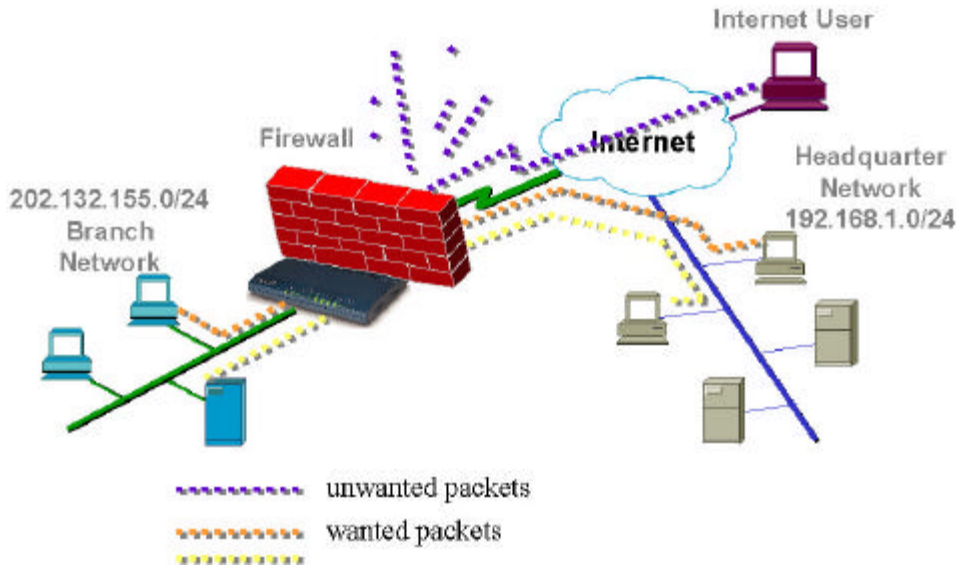
➢ Introduction

This configuration note explains how to configure the Prestige as the Internet firewall to allow all packet from headquarter through Internet, but would like to setup an Internet firewall to block other intrusion.

➢ Configuration

The Prestige 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
- ✓ Allow TCP, UDP traffic to ports > 1023
- ✓ Allow HTTP, SMTP, NNTP, DNS
- ✓ Block everything else inbound from the Internet



➢ Example

The procedure for configuring this filter is as follows.

- ✓ Create a filter set in Menu 21, e.g., set 1
- ✓ Create three filter rules in Menu 21.1.1, Menu 21.1.2, Menu 21.1.3
  - ❖ Rule 1- Allow all packet from headquarter network 192.168.1.0/24
  - ❖ Rule 2- Allow ICMP (including PING)
  - ❖ Rule 3- Allow UDP traffic to port > 1023
  - ❖ Rule 4- Allow TCP traffic to ports >1023
  - ❖ Rule 5- Allow the DNS request (if there is any DNS server running inside the branch network) and block all other packets
- ✓ Apply the filter set in remote node, Menu 11

✓ Create a filter set in Menu 21, e.g., set 1

```
                Menu 21 - Filter Set Configuration

Filter                              Filter
Set #    Comments                   Set #    Comments
------ ----------------             -----  ----------------
  1    Firewall                       7    _________________
  2    _________________              8    _________________
  3    _________________              9    _________________
  4    _________________             10    _________________
  5    _________________             11    _________________
  6    _________________             12    _________________

              Enter Filter Set Number to Configure= 0
              Edit Comments=
              Press ENTER to Confirm or ESC to Cancel:
```

✓ Create three filter rules in Menu 21.1.1, Menu 21.1.2, Menu 21.1.3

❖ Rule 1- Allow all packet from headquarter network 192.168.1.0/24

```
              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= No
                More= No          Log= None
                Action Matched= Forward
                Action Not Matched= Check Next Rule

            Press ENTER to Confirm or ESC to Cancel:
```

❖ Rule 2- Allow ICMP (including PING)

Menu 21.1.2 - TCP/IP Filter Rule

Filter #: 1,1
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= No
More= No Log= None
Action Matched= **Forward**
Action Not Matched= **Check Next Rule**

Press ENTER to Confirm or ESC to Cancel:

❖ Rule 3- Allow UDP traffic to port > 1023

Menu 21.1.3 - 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 #= **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= **Check Next Rule**

Press ENTER to Confirm or ESC to Cancel:

❖ Rule 4- Allow TCP traffic to ports >1023

```
Menu 21.1.4 - TCP/IP Filter Rule

        Filter #: 1,1
        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= Check Next Rule

    Press ENTER to Confirm or ESC to Cancel:
```

❖ Rule 5- Allow the DNS request (if there is any DNS server running inside the branch network) and block all other packets

```
        Menu 21.1.5 - 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 #= 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= Drop

    Press ENTER to Confirm or ESC to Cancel:
```

Then the filter rule summary in Menu 21 will look like as follows.

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	N
5	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=53	N	F	D

Sometimes Internet applications such as Video conference need to use the UDP server port, then you have to be careful in setting up the firewall filter. After you have finished the above filter set, you have to apply it in the **'Input Filter Set'** field in the remote node that is connecting to the ISP or the remote node.

Menu 11.5 - Remote Node Filter

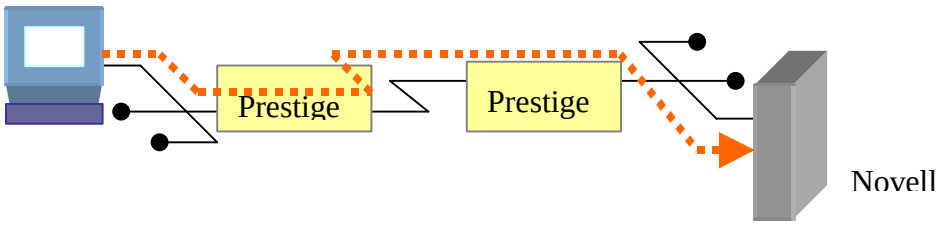
Input Filter Sets:
protocol filters=**1**
device filters=
Output Filter Sets:
protocol filters=
device filters=
Call Filter Sets:
protocol filters=
device filters=

IPX Filter Example

- Introduction

  This example shows you how to configure the protocol-dependent parameters for an IPX filter. In the case, a Windows 95 client always triggers the call to the remote node. From Menu 24.1 we know the packet is the IPX packet. And we would like to configure a call filter to prevent these unnecessary calls.

- Configuration



The packet captured in Menu 24.1 is as below.

LAN Packet Which Triggered Last Call: (Type: IPX)
FF FF 00 29 01 (11) (00 00 00 01) (00 00 00 00 00 01) (04 51)
(00 00 00 03) (00 60 94 AE A0 3E) 40 04 22 22 10 03 00 00 16 00 02 14 05

IPX packet type = 11 (11h for NCP)
Destination network number= 00 00 00 01 (1 for Novell server)
Destination node number=00 00 00 00 00 01 (1 for Novell server)
Destination socket number=0451 (0451 for NCP)

Source network number= 00 00 00 03 (Win95 network number)
Source node number=00 60 94 AE A0 3E
Source socket number, do not care, because it can be any socket number

After the above data is collected, you are ready to configure the IPX filter rule in Menu 21.

```
Menu 21.2.1 - IPX Filter Rule

Filter #: 2,1
Filter Type= IPX Filter Rule
Active= Yes
IPX Packet Type= 11
Destination: Network #= 00000001
        Node #= 000000000001
        Socket #= 0451
        Socket # Comp= Equal
   Source: Network #= 00000003
        Node #= 006094aea03e
        Socket #= 0000
        Socket # Comp= None
Operation= N/A
More= No        Log= None
Action Matched= Drop

Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
```

After the filter rule is finished, you can apply it to the **'Call Filter Sets'** in Menu 11.5. Please set the **'Edit Filter Sets'** in Menu 11.1 to **'Yes'** to enter to the Menu 11.5

```
Menu 11.1 - Remote Node Profile

Rem Node Name= p2            Route= IP
Active= Yes                  Bridge= No

Call Direction= Outgoing     Edit PPP Options= No
Incoming:                    Rem IP Addr= 0.0.0.0
  Rem Login= N/A             Edit IP/IPX/Bridge= No
  Rem Password= N/A          Telco Option:
  Rem CLID= N/A                Allocated Budget(min)= 0
  Call Back= N/A               Period(hr)= 0
Outgoing:                    Transfer Type= 64K
  My Login= zyxel             Nailed-Up Connection= No
  My Password= ********      Session Options:
  Authen= CHAP/PAP             Edit Filter Sets= Yes
  Pri Phone #= 4125678         Idle Timeout(sec)= 300
  Sec Phone #=

        Press ENTER to Confirm or ESC to Cancel:
```

```
Menu 11.5 - Remote Node Filter

      Input Filter Sets:
        protocol filters=
          device filters=
      Output Filter Sets:
        protocol filters=
          device filters=
      Call Filter Sets:
        protocol filters= 1
          device filters=
```

PPTP Tunneling

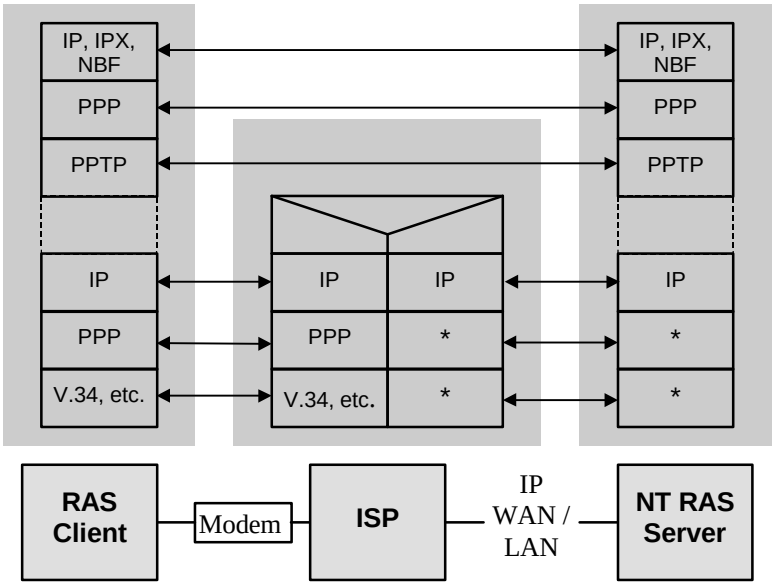
Configuring Prestige to route the PPTP packets in SUA mode

➢ Introduction

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself.

In order to run the Windows9x PPTP client, you must be able to establish an IP connection with a tunnel server such as the Windows NT Server 4.0 Remote Access Server.

Windows Dial-Up Networking uses the Internet standard Point-to-Point (PPP) to provide a secure, optimized multiple-protocol network connection over dialed telephone lines. All data sent over this connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, NetBEUI and IPX) can be run correctly. Windows NT Domain Login level security is preserved even across the Internet.



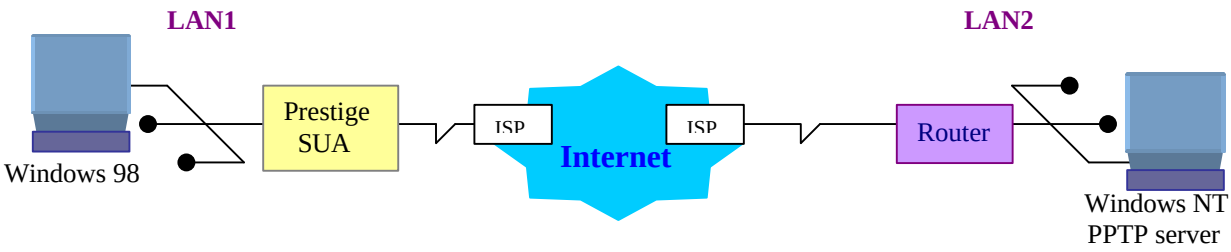
Window95 PPTP Client / Internet / NT RAS Server Protocol Stack

PPTP appears as new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the Dial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial-up adapter that provides PPP support for the analog or ISDN modem.

The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

➢ Configuration

This application note explains how to establish a PPTP connection to a remote private network in the Prestige SUA case. For RAS 2.20, all PPTP packets can be forwarded to the internal PPTP Server (WinNT server) in the SUA case. The port number of the PPTP has to be entered in the SMT Menu 15
for Prestige to forward to the appropriate private IP address of Windows NT server. See the configuration for Prestige SUA application below.



➢ Example

The following example walks through the case of dialing to an ISP via Prestige and then establishing a tunnel to a private network. There will be three items that you need to set up for PPTP application, these are PPTP server (WinNT), PPTP client (Win9x) and Prestige.

✓ PPTP server setup (WinNT)

- ❖ Add the VPN service from Control Panel>Network
- ❖ Add an user account for PPTP logged on user
- ❖ Enable RAS port
- ❖ Select the network protocols from RAS such as IPX, TCP/IP NETBUEI
- ❖ Set the Internet gateway to Prestige

✓ PPTP client setup (Win9x)

- ❖ Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the Prestige's Internet IP address for logging to NT RAS server.
- ❖ Set the Internet gateway to the router that is connecting to ISP

✓ Prestige router setup

Before making a VPN connection from Win9x to WinNT server, you need to connect Prestige router to your ISP first. Please check the following settings when connecting to your ISP.

- ❖ *General Setup in SMT Menu 1*-enter the system information.
- ❖ *ISDN Setup in SMT Menu 2*-enter your ISDN number
- ❖ *Ethernet Setup in SMT Menu 3*-enter the IP address of the Prestige
- ❖ *Internet Access Setup in SMT Menu 4*-enter the ISP phone number and ISP account
- ❖ *Multiple Server Configuration in SMT Menu 15*-enter the IP address of the PPTP server (WinNT server)

1. Ethernet Setup in SMT Menu 3

```
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= 192.168.10.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
```

2. Internet Access Setup in Menu 4

```
Menu 4 - Internet Access Setup

  ISP's Name= hinet
  Pri Phone #= 4125678
  Sec Phone #=
  My Login= test
  My Password= ********
  Single User Account= Yes
    IP Addr= 0.0.0.0

  Telco Options:
  Transfer Type= 64K

  Multilink= Off
  Idle Timeout= 300

Do you wish to perform the Internet Setup Test [y/n]:
```

- **Pri Phone#=**, enter the phone number for dialing to ISP
- **My Login** and **My Password** are the login information provided by ISP.
- Since you have a single user Internet account**, Single User Account** should be set to **'Yes'**.
- **IP Addr=** , enter the IP address your ISP assigns to you or enter **'0.0.0.0'** if the IP is dynamically assigned by ISP server.

After saving this menu, you will be asked if you want to perform an Internet connection test. Select **'Yes'** to perform the test. If the test fails, please check again the above settings or refer to the User's Manual Troubleshooting section for correction action.

3. Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP

```
        Menu 15 - Multiple Server Configuration

              Port #        IP  Address
              ------        ---------------
            1.Default       0.0.0.0
            2. 1723         192.168.10.5
            3. 21           192.168.10.3
            4. 0            0.0.0.0
            5. 0            0.0.0.0
            6. 0            0.0.0.0
            7. 0            0.0.0.0
            8. 0            0.0.0.0

                Press ENTER to Confirm or ESC to Cancel:

HTTP:80  FTP:21  TELNET:23  MAIL:25  PPTP:1723
```

After the Menu 4 is saved, a remote node will be created in Menu 11 automatically. You can do more advanced configuration options to this remote node from the Menu 11.

```
Menu 11 - Remote Node Setup

        1. hinet (ISP)
        2. _________
        3. _________
        4. _________
```

```
        Menu 11.1 - Remote Node Profile

Rem Node Name= hinet          Route= IP
Active= Yes                   Bridge= No

Call Direction= Outgoing      Edit PPP Options= No
Incoming:                     Rem IP Addr= 0.0.0.0
  Rem Login= N/A              Edit IP/IPX/Bridge= No
  Rem Password= N/A           Telco Option:
  Rem CLID= N/A                 Allocated Budget(min)= 0
  Call Back= N/A                Period(hr)= 0
Outgoing:                     Transfer Type= 64K
  My Login= test              Nailed-Up Connection= No
  My Password= ********       Session Options:
  Authen= CHAP/PAP              Edit Filter Sets= No
  Pri Phone #= 4125678          Idle Timeout(sec)= 100
  Sec Phone #=

        Press ENTER to Confirm or ESC to Cancel:
```

You can test the connection from the **'Internet Set Test'** in Menu 24.4.11.

```
Menu 24.4 - System Maintenance - Diagnostic

ISDN                          System
  1. Hang Up B1 Call            21. Reboot System
  2. Hang Up B2 Call            22. Command Mode
  3. Reset ISDN
  4. ISDN Connection Test
  5. Manual Call

TCP/IP
  11. Internet Setup Test
  12. Ping Host
                Enter Menu Selection Number:

          Manual Call Remote Node= N/A
          Host IP Address= N/A
```

After you finish the above settings, you can ping to remote Win9x client from WinNT. This ping command is used to demonstrate that remote Win9x can be reached across the Internet. If the Internet connection between two LANs is running, you are ready to place a VPN call now from remote Win9x client.

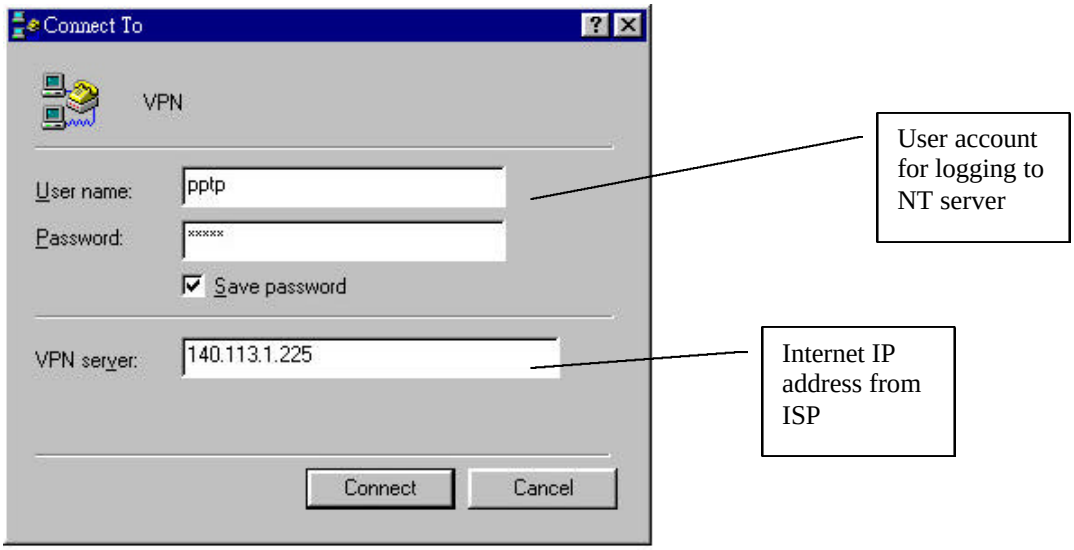
For example:

C:\ping 203.66.113.2

When a dial-up connection to ISP is established, a default gateway is assigned to router traffic through that connection. Therefore, the output below shows the default gateway of the Win95 client after the dial-up connection has been established.

Before making a VPN connection from Win9x client to NT server, you need to know the exact Internet IP address that the ISP assigns to Prestige router in SUA mode and enter this IP address in the VPN dial-up dialog box. You can check this Internet IP address from SMT Menu 24.1. If the Internet IP address is a fixed IP address provided by ISP in SUA mode, then you can always use this IP address for reaching the VPN server.

In the following example, the IP address **'140.113.1.225'** is dynamically assigned from ISP to Prestige running the SUA application. You must enter this IP address in the **'VPN Server'** dialog box for reaching the PPTP server. After the VPN link is established, you can start the network protocol application such as IP, IPX and NetBEUI.



Using ISDN Protocol Analyzer

EPAPC Tool

Introduction

Prestige EPAPC tool is a DOS utility that interprets the dump of the ISDN D channel signaling from Prestige. An ISDN call connection failure can be diagnosed by using Prestige's ISDN embedded protocol analyzer (EPA). The **cause code** in the EPA log can also help us to diagnose an ISDN call. The EPAPC program can be found in the supporting disk.

ISDN Protocol Analyzer

You must connect the Prestige to a terminal program via the serial port to capture the EPA. The EPA will not operate by Telnet. The steps for enabling the EPA are as follows:

1. Enter to SMT Menu 11 and note which node **N** you will be dialing
2. Enter to SMT Menu 24.8
3. Enable the EPA capture capability:

   Prestige>isdn fw ana on

4. Manually dial to remote node N

   Prestige>dev dial N (N is the node number in Menu 11)

Example:

```
Prestige> dev dial 1
Start dialing for node <hinet>...
### Hit any key to continue.###
$$$ DIALING dev=2 ch=0.....
$$$ OUTGOING-CALL phone(4125678)
```

5. Wait for all progress messages, and manually drop the call:

   Prestige>dev channel drop [bri0|bri1] (bri0 for B1 channel, bri1 for B2 channel)

6. Turn off the EPA by:

   Prestige>isdn fw ana off

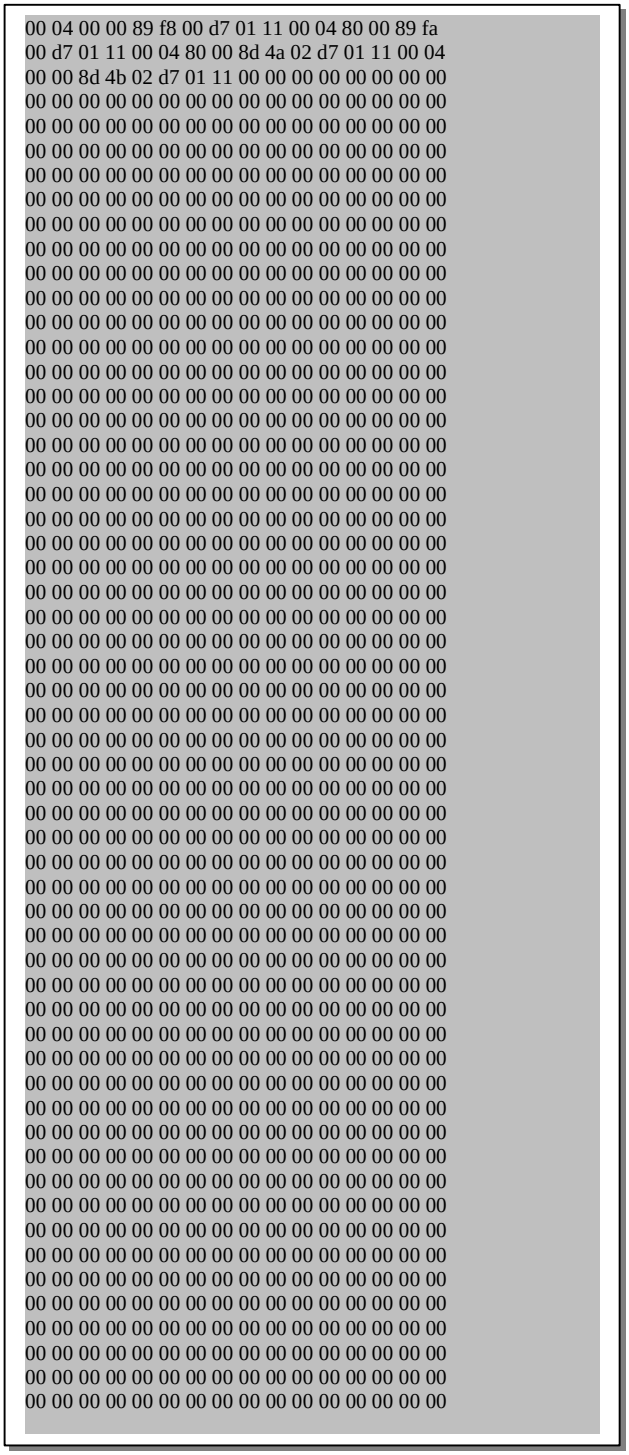
7. Dump the EPA by:

Prestige>isdn fw ana dump

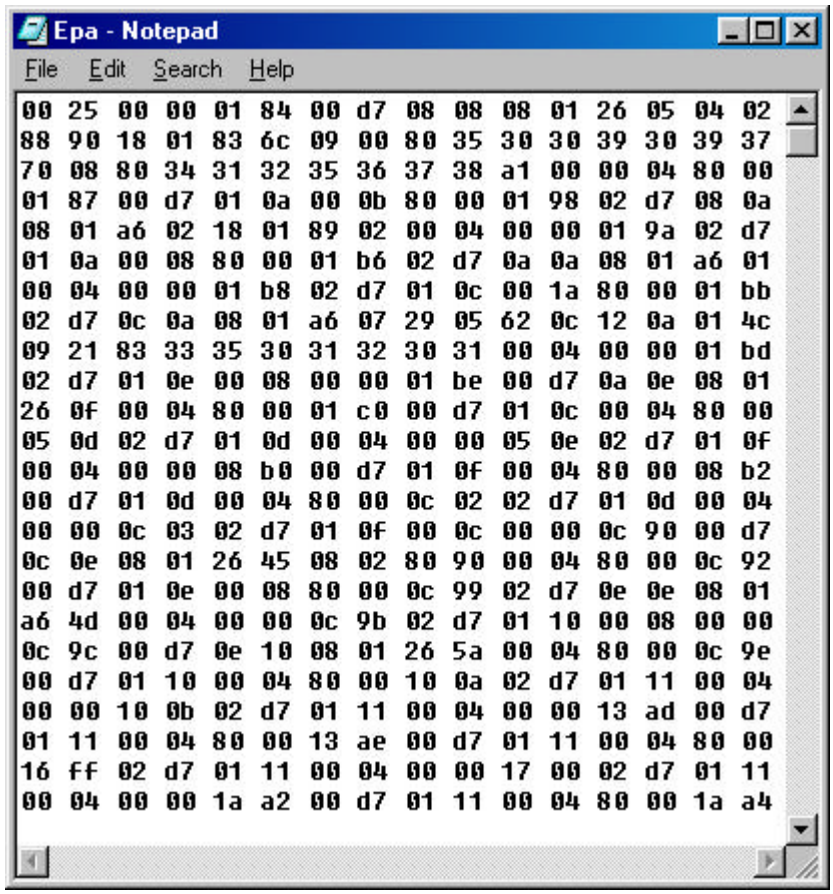
The trace appears on the screen as in the following example. Press **Enter** key to dump the entire trace.

Example:

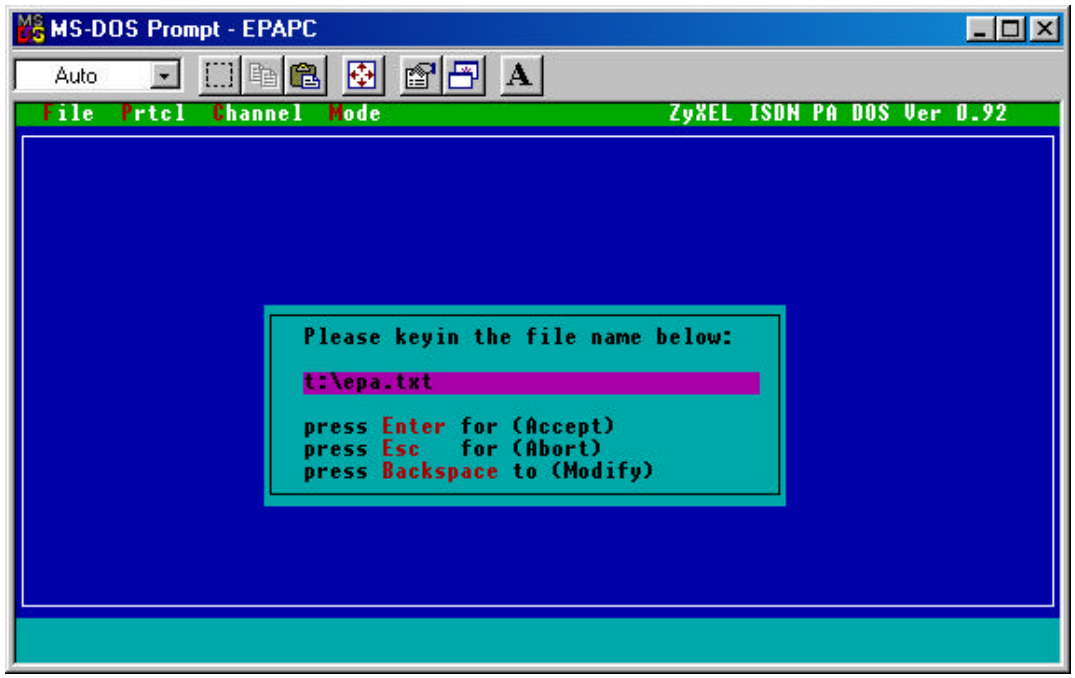
```
Prestige> isdn fw ana dump
00 25 00 00 01 84 00 d7 08 08 08 01 26 05 04 02
88 90 18 01 83 6c 09 00 80 35 30 30 39 30 39 37
70 08 80 34 31 32 35 36 37 38 a1 00 00 04 80 00
01 87 00 d7 01 0a 00 0b 80 00 01 98 02 d7 08 0a
08 01 a6 02 18 01 89 02 00 04 00 00 01 9a 02 d7
01 0a 00 08 80 00 01 b6 02 d7 0a 0a 08 01 a6 01
00 04 00 00 01 b8 02 d7 01 0c 00 1a 80 00 01 bb
02 d7 0c 0a 08 01 a6 07 29 05 62 0c 12 0a 01 4c
09 21 83 33 35 30 31 32 30 31 00 04 00 00 01 bd
02 d7 01 0e 00 08 00 00 01 be 00 d7 0a 0e 08 01
26 0f 00 04 80 00 01 c0 00 d7 01 0c 00 04 80 00
05 0d 02 d7 01 0d 00 04 00 00 05 0e 02 d7 01 0f
00 04 00 00 08 b0 00 d7 01 0f 00 04 80 00 08 b2
00 d7 01 0d 00 04 80 00 0c 02 02 d7 01 0d 00 04
00 00 0c 03 02 d7 01 0f 00 0c 00 00 0c 90 00 d7
0c 0e 08 01 26 45 08 02 80 90 00 04 80 00 0c 92
00 d7 01 0e 00 08 80 00 0c 99 02 d7 0e 0e 08 01
a6 4d 00 04 00 00 0c 9b 02 d7 01 10 00 08 00 00
0c 9c 00 d7 0e 10 08 01 26 5a 00 04 80 00 0c 9e
00 d7 01 10 00 04 80 00 10 0a 02 d7 01 11 00 04
00 00 10 0b 02 d7 01 11 00 04 00 00 13 ad 00 d7
01 11 00 04 80 00 13 ae 00 d7 01 11 00 04 80 00
16 ff 02 d7 01 11 00 04 00 00 17 00 02 d7 01 11
00 04 00 00 1a a2 00 d7 01 11 00 04 80 00 1a a4
00 d7 01 11 00 04 80 00 1d f4 02 d7 01 11 00 04
00 00 1d f5 02 d7 01 11 00 04 00 00 21 97 00 d7
01 11 00 04 80 00 21 99 00 d7 01 11 00 04 80 00
24 ea 02 d7 01 11 00 04 00 00 24 eb 02 d7 01 11
00 04 00 00 28 8d 00 d7 01 11 00 04 80 00 28 8f
00 d7 01 11 00 04 80 00 2b df 02 d7 01 11 00 04
00 00 2b e0 02 d7 01 11 00 04 00 00 2f 82 00 d7
01 11 00 04 80 00 2f 84 00 d7 01 11 00 04 80 00
32 d4 02 d7 01 11 00 04 00 00 32 d5 02 d7 01 11
00 04 00 00 36 77 00 d7 01 11 00 04 80 00 36 79
00 d7 01 11 00 04 80 00 39 ca 02 d7 01 11 00 04
00 00 39 cb 02 d7 01 11 00 04 00 00 3d 6d 00 d7
01 11 00 04 80 00 3d 6f 00 d7 01 11 00 04 80 00
40 bf 02 d7 01 11 00 04 00 00 40 c0 02 d7 01 11
00 04 00 00 44 62 00 d7 01 11 00 04 80 00 44 64
00 d7 01 11 00 04 80 00 47 b5 02 d7 01 11 00 04
00 00 47 b6 02 d7 01 11 00 04 00 00 4b 58 00 d7
01 11 00 04 80 00 4b 5a 00 d7 01 11 00 04 80 00
4e aa 02 d7 01 11 00 04 00 00 4e ab 02 d7 01 11
00 04 00 00 52 4d 00 d7 01 11 00 04 80 00 52 4f
00 d7 01 11 00 04 80 00 55 9f 02 d7 01 11 00 04
00 00 55 a0 02 d7 01 11 00 04 00 00 59 42 00 d7
01 11 00 04 80 00 59 44 00 d7 01 11 00 04 80 00
5c 95 02 d7 01 11 00 04 00 00 5c 96 02 d7 01 11
00 04 00 00 60 38 00 d7 01 11 00 04 80 00 60 3a
00 d7 01 11 00 04 80 00 63 8a 02 d7 01 11 00 04
00 00 63 8b 02 d7 01 11 00 04 00 00 67 2d 00 d7
01 11 00 04 80 00 67 2f 00 d7 01 11 00 04 80 00
6a 7f 02 d7 01 11 00 04 00 00 6a 80 02 d7 01 11
00 04 00 00 6e 22 00 d7 01 11 00 04 80 00 6e 24
00 d7 01 11 00 04 80 00 71 75 02 d7 01 11 00 04
00 00 71 76 02 d7 01 11 00 04 00 00 75 18 00 d7
01 11 00 04 80 00 75 1a 00 d7 01 11 00 04 80 00
78 6a 02 d7 01 11 00 04 00 00 78 6b 02 d7 01 11
00 04 00 00 7c 0d 00 d7 01 11 00 04 80 00 7c 0e
00 d7 01 11 00 04 80 00 7f 5f 02 d7 01 11 00 04
00 00 7f 60 02 d7 01 11 00 04 00 00 83 02 00 d7
01 11 00 04 80 00 83 04 00 d7 01 11 00 04 80 00
86 55 02 d7 01 11 00 04 00 00 86 56 02 d7 01 11
```


00 04 00 00 89 f8 00 d7 01 11 00 04 80 00 89 fa
00 d7 01 11 00 04 80 00 8d 4a 02 d7 01 11 00 04
00 00 8d 4b 02 d7 01 11 00 00 00 00 00 00 00 00

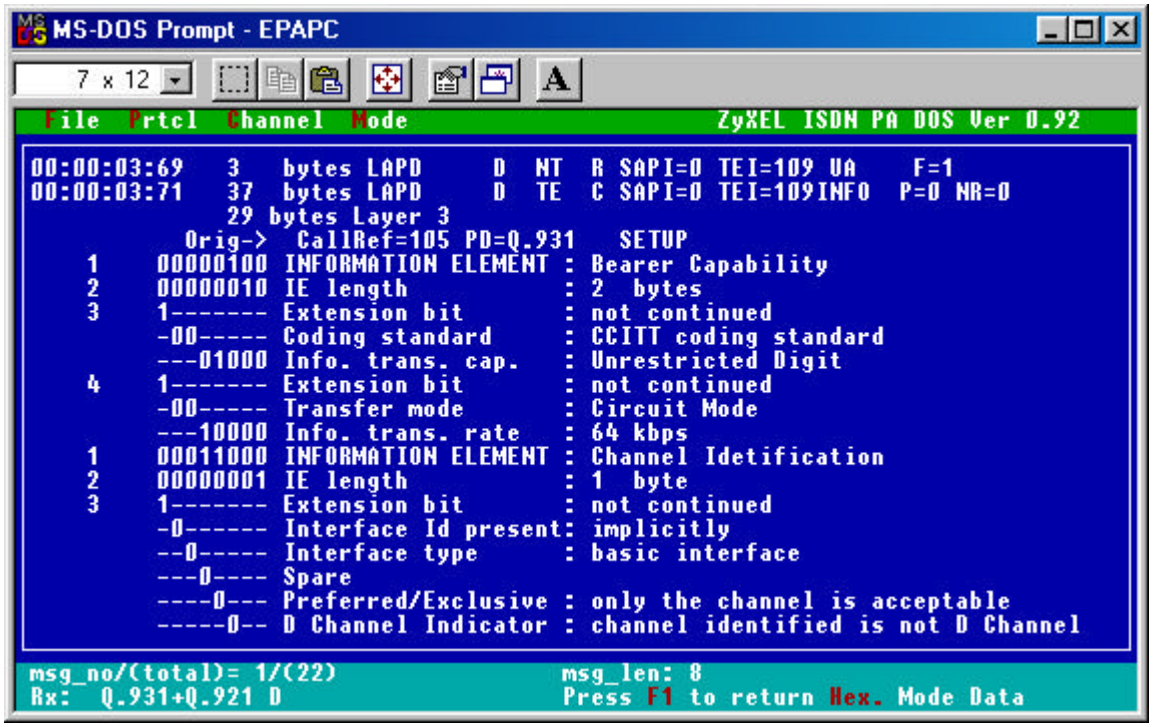
8. Copy and Paste the entire trace to an Editor and save it as a text file



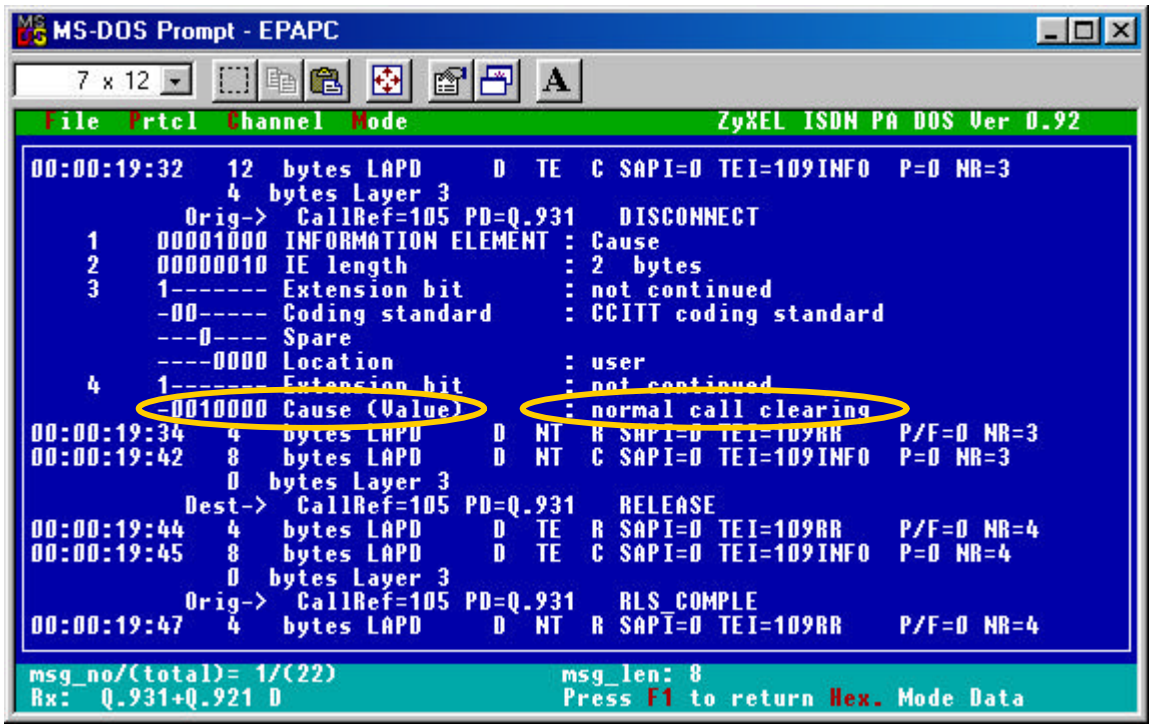
9. Run the EPAPC program in DOS mode
10. Load the saved file



11. The EPAPC will interpret the trace as following. Use **PageUP** and **PageDown** to inspect the entire trace



12. The **Cause Code** in the Disconnect message will help us to diagnose the ISDN connection problem



Using PPP Protocol Analyzer

——— ZPKTTOOL Tool

Introduction

The Prestige supports the trace of PPP log, that we can diagnose from the trace by referring to the **PPP numbers** or use the ZPKTTOOL to interpret for us.

Prestige ZPKTTOOL tool is a DOS utility that interprets the dump of the PPP log in Prestige. A PPP call connection failure can be diagnosed by using Prestige's PPP protocol analyzer. The ZPKTTOOL program can be found in the supporting disk.

PPP Protocol Analyzer

You must connect the Prestige to a terminal program via the serial port to capture the PPP log. The PPP log will not operate by Telnet. The steps for capturing the PPP log are as follows:

1. Enter to SMT Menu 11 and note which node **N** you will be dialing
2. Enter to SMT Menu 24.8
3. Enable the PPP trace capability by:

   Prestige>sys trcl cl
   Prestige>sys trcl sw on
   Prestige>sys trcp sw on

4. Manually dial to remote node N

   Prestige>dev dial N (N is the node number in Menu 11)

Example:

```
Prestige> dev dial 1
Start dialing for node <hinet>...
### Hit any key to continue.###
$$$ DIALING dev=2 ch=0.....
$$$ OUTGOING-CALL phone(4125678)
$$$ CALL CONNECT speed<64000> type<2>
chan<0>
$$$ LCP opened
$$$ PAP sending user/pswd
$$$ IPCP negotiation started
$$$ CCP stopped
$$$ IPCP opened
```

5. Wait for all progress messages, and manually drop the call:

Prestige>dev channel drop [bri0|bri1] (bri0 for B1 channel, bri1 for B2 channel)

6. Turn off the PPP trace by:

Prestige>sys trcl sw off
Prestige>sys trcp sw off

7. Dump the PPP log by:

Prestige>sys trcl disp

The trace appears on the screen as in the following example. Press **Enter** key to dump the entire trace.

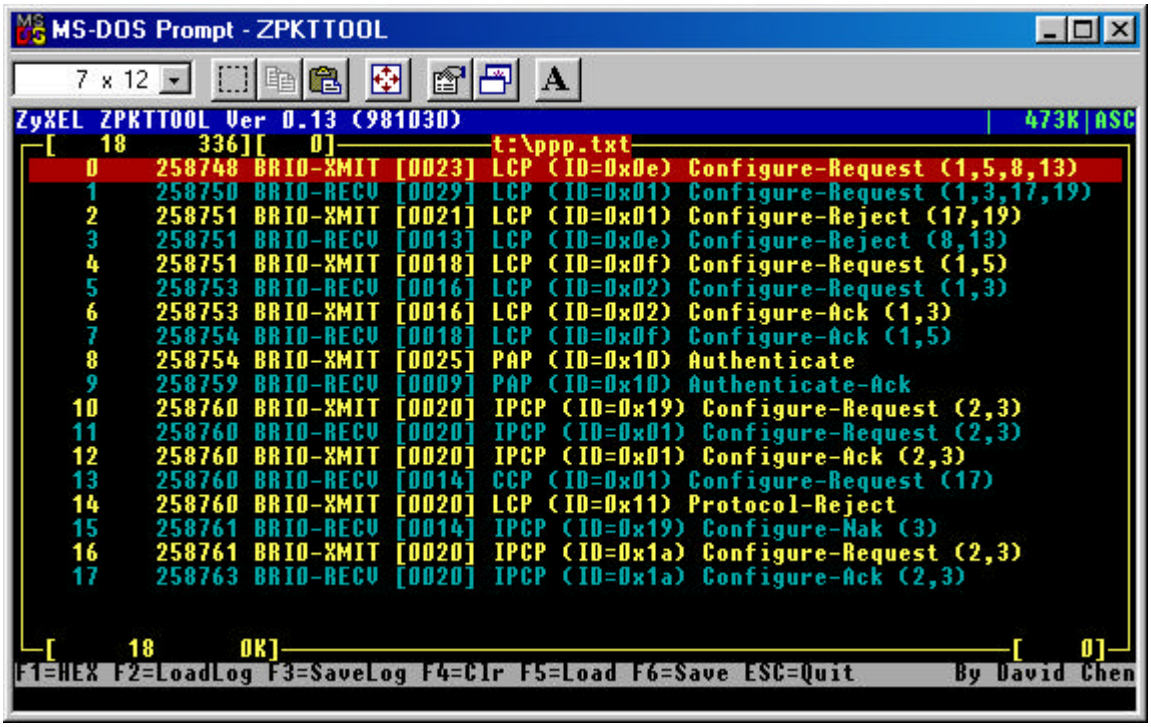
Example:

```
Prestige> dev chan drop bri0
Prestige> sys trcl sw off
Prestige> sys trcp sw off
Prestige> sys trcl disp
 87     258407 PP08 DIALING dev=2 ch=0.....
 88     258407 PP08 OUTGOING-CALL phone(4125678)
 89     258470 PP08 CALL CONNECT speed<64000> type<2> chan<0>
 90     258471 PP09 ebp=7ea690,seqNum=5c bri0-XMIT len:23 call=4
0000: ff 03 c0 21 01 0d 00 13 01 04 05 f4 05 06 00 03
0010: f1 a6 08 02 0d 03 06
 91     258748 PP09 ebp=7ea6c4,seqNum=5d bri0-XMIT len:23 call=4
0000: ff 03 c0 21 01 0e 00 13 01 04 05 f4 05 06 00 03
0010: f1 a6 08 02 0d 03 06
 92     258750 PP09 ebp=7ea6f8,seqNum=5e bri0-RECV len:29 call=4
0000: ff 03 c0 21 01 01 00 19 01 04 05 f4 03 04 c0 23
0010: 11 04 05 f4 13 09 03 00 c0 7b 72 cf 08
 93     258751 PP09 ebp=7ea72c,seqNum=5f bri0-XMIT len:21 call=4
0000: ff 03 c0 21 04 01 00 11 11 04 05 f4 13 09 03 00
0010: c0 7b 72 cf 08
 94     258751 PP09 ebp=7ea760,seqNum=60 bri0-RECV len:13 call=4
0000: ff 03 c0 21 04 0e 00 09 08 02 0d 03 06
 95     258751 PP09 ebp=7e9dd4,seqNum=61 bri0-XMIT len:18 call=4
0000: ff 03 c0 21 01 0f 00 0e 01 04 05 f4 05 06 00 03
0010: f1 a6
 96     258753 PP09 ebp=7e9e08,seqNum=62 bri0-RECV len:16 call=4
0000: ff 03 c0 21 01 02 00 0c 01 04 05 f4 03 04 c0 23
 97     258753 PP09 ebp=7e9e3c,seqNum=63 bri0-XMIT len:16 call=4
0000: ff 03 c0 21 02 02 00 0c 01 04 05 f4 03 04 c0 23
 98     258754 PP09 ebp=7e9e70,seqNum=64 bri0-RECV len:18 call=4
0000: ff 03 c0 21 02 0f 00 0e 01 04 05 f4 05 06 00 03
0010: f1 a6
 99     258754 PP09 LCP opened
100     258754 PP09 PAP sending user/pswd
101     258754 PP09 ebp=7e9ea4,seqNum=65 bri0-XMIT len:25 call=4
0000: ff 03 c0 23 01 10 00 15 07 7a 79 78 65 6c 72 64
0010: 08 70 72 65 73 74 69 67 65
102     258759 PP09 ebp=7e9ed8,seqNum=66 bri0-RECV len:9 call=4
0000: ff 03 c0 23 02 10 00 05 00
103     258759 PP09 IPCP negotiation started
104     258760 PP09 ebp=7e9f0c,seqNum=67 bri0-XMIT len:20 call=4
```

```
105     258760 PP09 ebp=7e9f40,seqNum=68 bri0-RECV len:20 call=4
 0000: ff 03 80 21 01 01 00 10 02 06 00 2d 0f 01 03 06
 0010: a8 5f 43 2b
106     258760 PP09 ebp=7e9f74,seqNum=69 bri0-XMIT len:20 call=4
 0000: ff 03 80 21 02 01 00 10 02 06 00 2d 0f 01 03 06
 0010: a8 5f 43 2b
107     258760 PP09 ebp=7e9fa8,seqNum=6a bri0-RECV len:14 call=4
 0000: ff 03 80 fd 01 01 00 0a 11 06 00 01 01 03
108     258760 PP09 ebp=7e9fdc,seqNum=6b bri0-XMIT len:20 call=4
 0000: ff 03 c0 21 08 11 00 10 80 fd 01 01 00 0a 11 06
 0010: 00 01 01 03
109     258761 PP09 ebp=7ea010,seqNum=6c bri0-RECV len:14 call=4
 0000: ff 03 80 21 03 19 00 0a 03 06 a3 1f f4 2e
110     258761 PP09 ebp=7ea044,seqNum=6d bri0-XMIT len:20 call=4
 0000: ff 03 80 21 01 1a 00 10 02 06 00 2d 0f 00 03 06
 0010: a3 1f f4 2e
111     258763 PP09 ebp=7ea078,seqNum=6e bri0-RECV len:20 call=4
 0000: ff 03 80 21 02 1a 00 10 02 06 00 2d 0f 00 03 06
 0010: a3 1f f4 2e
112     258763 PP09 IPCP opened
113     260465 PP09 FSM_DOWN state= 9
114     260465 PP09 LCP closed
115     260465 PP09 FSM_DOWN state= 9
116     260465 PP09 IPCP closed
117     260465 PP09 FSM_DOWN. state=1
118     260465 PP09 FSM_DOWN state= 1
119     260465 PP09 FSM_DOWN. state=1
120     260465 PP09 FSM_DOWN state= 0
121     260465 PP09 FSM_DOWN. state=0
122     260465 PP09 FSM_DOWN state= 0
123     260465 PP09 FSM_DOWN. state=0
124     260465 PP09 FSM_DOWN state= 0
125     260465 PP09 FSM_DOWN. state=0
126     260465 PP09 FSM_DOWN. state=1
127     260465 PP09 PPP down chan<0>, 0
Program Trace Switch OFF
Packet Trace Switch OFF
Prestige>
```

8. Copy and paste the trace to an editor and save it as a text file

9. Run the ZPKTTOOL program to interpret the PPP log



Prestige Configuration Transfer Tool

1. Introduction

Prestige Configuration Transfer (PCT) Tool is a stand-alone Java based program that runs on PC/Win95 to transfer configuration data through TFTP protocol. PCT can only work with Prestige ZyNOS based firmware release (Release 2.10 & above).
When PWC is installed from CD, PCT and the required JRE (Java Run-Time Environment) will also be installed.

2. Function

PCT supports file transfer either through WAN or LAN. After PCT is clicked. PCT will use HDAP protocol to detect a list of Prestige in the local network. After selecting the Prestige and entering a password, a user will have several choices:

- Restore Configuration from a Binary file (romfile0)
- Backup Configuration into a Binary file (romfile0)
- Update firmware
- Restore Configuration from a Text file
- Backup Configuration to a Text file

- After PCT is clicked, if there is only one Prestige in the local network, this Prestige will be selected automatically. PCT will try the default password “1234” first, if this fails, PCT will ask the user to enter a password.
- If there is no Prestige detected in the local network, A user can enter the IP address, then password to start PCT functions. By this way, PCT will connect to a Prestige in a remote site via WAN.
- Updating firmware is only supported on some restricted models. That is: the models with 2M DRAM(P100MH, P100IH)
- The “restore” function has an option to execute device initialization and ISP connection as well as an ISDN loop back test.
- When PCT is executed, progress will be recorded in a default log file. The log file will include the progress of download, upload, device initialization, and ppp negotiation. Each record in the log file should have data & time. The name of the log file is log.txt and will be stored in the working directory.

3. Prestige Configuration binary/text conversion

There are over 2000 fields in Prestige Configuration. PCT HAS NO INTENTION TO COVER ALL CONFIGURATION FIELDS. PCT only covers fields that are required to set up an Internet connection. The specific fields that will be converted are contained within the program itself. If new fields are to be added, the program will have to be edited and rebuilt.

Backup Configuration to a Text file

A user must enter a directory path. PCT will upload spt binary file first. PCT will convert the binary file into a text file.

Restore configuration from a Text file.

A user must enter a directory path. PCT will use a base Spt binary file. Then, PCT will convert data in the text file into a working binary file and download the working binary file to Prestige. The name of the binary file is the first comment in the text file.

After downloading is completed, a user can have an option to initialize ISDN line and execute Internet connection.

Pre-Configuration

ISP can edit a configuration text file for a customer; store the text file and an associated binary spt file in a diskette. Then distribute to his customer a diskette, together with Prestige package.

4. Format of SPT description file

Example of a text file

/* wan.bin

/ System

1234 : System Password : [0,4,0]

/ WAN Slot

5 : Port Speed<0(2.4K
) | 1(9.6K) | 2(19.2K) | 3(38.4K) | 4(57.6K) | 5(115.2K) | 6(230.4K) | 7(
460K) > : [2,8,2]
at&fs0=02s95=1 : AT Init String : [2,9,2]
0 : Call Direction<0(Outgoing) | 1(Incoming) | 2(Both) > : [2,10,2]

/ Ethernet Slot

204.247.203.174 : IP Address : [2,0,0]
26 : IP Subnet Mask : [2,1,0]
1 : DHCP<0(None) | 1(Server)> : [0,0,0]
204.247.203.174 : Client IP Pool Starting Address : [0,1,0]
1.1.1.1 : Primary DNS Server : [0,2,0]
2.2.2.2 : Secondary DNS Server : [0,3,0]

/ ISP Remote Node

bestCom : ISP's Name : [7,0,0]
1234 : Pri Phone # : [7,1,0]
2234 : Sec Phone # : [7,2,0]
sminc : My Login : [7,3,0]
CewSH2px : My Password : [7,4,0]
1 : Single User Account<0(No) | 1(Yes)> : [7,5,0]
300 : Idle Timeout(sec) : [7,6,0]
0 : Compression<0(No) | 1(Yes)> : [7,7,0]
0 : Encapsulation<0(Standard PPP) | 1(CISCO PPP)> : [7,8,0]
0 : Multilink<0(None) | 1(BOD) | 2(Always)> : [7,10,0]

Format of a text file

Zzzzz : yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy : [a,b,c]

Zzz
The value of a field

Yyy
Description of a field

[a,b,c]
These three numbers are used to identity a field. They cannot be modified. Otherwise, the field cannot be identified by PCT.

5. PCT Design Specs

Functionality

1) **Selecting the Prestige**
- The PCT will use the HDAP protocol to scan the LAN for available Prestiges. If only one is found, that one will automatically be selected for the user. If more than one is found, then the user will be able to choose one of them.
- If no Prestiges are found, PCT will ask the user to enter the IP address of the router.

2) **Logging on to the Prestige**
- In either case, once the Prestige is selected, PCT will assume the user is configuring a new Prestige and will first try to log on using the default password, 1234.
- If the default password fails, then the user will be prompted for the password.
- If the user enters an incorrect password, they can try again.

3) **Selecting a function**

- The following functions will be available to the user :
    - Restore Configuration from Binary File
    - Backup Configuration to Binary File
    - Update Firmware
    - Restore Configuration from Text File
    - Backup Configuration to Text File
    - Debugging Tools
- "Restore Configuration from Binary File" - This will allow the user to specify a binary file to transfer to the Prestige.
- "Backup Configuration to Binary File" - This will allow the user to save the configuration from the Prestige to the specified binary file.
- "Update Firmware" - This will allow the user to update the firmware on the Prestige by selecting an appropriate file. This function is limited to models with 2M DRAM (P100MH and P100IH).
- "Restore Configuration from Text File" - This will allow the user to specify a text file to transfer to the Prestige. The PCT will first convert this file into a binary file based on an SPT binary file in the specified directory.
- "Backup Configuration to Text File" - This will allow the user to save the configuration from the Prestige to the specified text file. The PCT will first upload the configuration as a binary file and convert this into the specified text file. The name of the binary file will be the name of the text file with the extension *.bin.
- "Debugging Tools" - This will contain various debugging tools.

4) **Executing the selected function**

- After the function is selected, PCT will execute the function.
- The user will be asked to enter the appropriate paths to the files they wish to transfer.
- A status bar will indicate the progress of the file transfer.

5) **After the function is executed**

- If the user selected to restore a configuration, they will have the option of initializing the line and executing an Internet connection to see if the settings are correct.
- A log file will be generated, and the name of the file will be log.txt.
- The log file will include the progress of download, upload, device initialization, and ppp negotiation. Each record in the log file will have data and time.

Supported configuration fields
(PCT is designed only to deal with configuration fields related to the user's ISP connection)

The following configuration fields are supported :

ISDN models

US	**DSS 1**
Switch Type	Data Call #
Phone # 1	Dial Prefix
SPID 1	
Phone # 2	
SPID 2	
LAN	**ISP**
IP Address	ISP Name
Subnet Mask	User Name
DHCP Server : y/n	Password
Starting IP Address (pool)	Primary Phone #
Primary DNS Server	Secondary Phone #
Secondary DNS Server	Single User Account : y/n
	MP : Both/Always/Off
System	Device Type (for devices w/ more than 1 port)
	Compression : y/n
System Password	

WAN/Modem models

WAN	**System**
Port #	System Password
Port Speed	
AT Command Init String	
Call Direction	
LAN	**ISP**
IP Address	ISP Name
Subnet Mask	User Name
DHCP Server : y/n	Password
Starting IP Address (pool)	Primary Phone #
Primary DNS Server	Secondary Phone #
Secondary DNS Server	Single User Account : y/n
	MP : Both/Always/Off
	Device Type (for devices w/ more than 1

	port)
	Compression : y/n

Design Information

The PCT will be designed and coded using Java. The code itself will be based on previous versions of PCT, PWC, and SPTGEN. The differences are that this version will use TFTP and will automatically translate between binary and text files. The program will consist of a main application window that will update depending on what the user is currently doing. Dialog boxes will be displayed when PCT needs to alert the user of something or to ask simple Yes/No questions.

PCT will be designed to make it as easy as possible for the user and to avoid user error. In the end, the application can be compiled to native Win 32 code or Java byte code. If Java code is used, PCT will have to be shipped with the appropriate JRE. If Win 32 code is used, PCT will have to be shipped with Symantec's Run Time Environment.

Protocols

PCT will use the TFTP protocol to transfer configuration files. A telnet session will be established first between the PCT and Prestige. Then, a TFTP session will be established to transfer the files. Once this is done, the TFTP session will end. Then, PCT will issue the CI command, *"sys spt save"*, before killing the telnet session.

PCT will use the same TFTP client implementation as PWC.

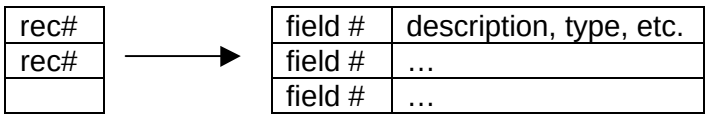
HDAP will be used to detect if there are any Prestiges on the network. If not, the user will have to manually enter an IP address.

Telnet will be used to communicate with the Prestige. For example, to send the password and to send any CI commands that are needed.

For more complete information on the internal data structures, see the file on how to Edit Configuration fields in PCT.

Description Table

The descriptions will be separated by their record number and each record will point to a list of entries for that type of record. The descriptions will be stored along with the offset and data type information. This will allow the information to be retrieved quickly using the record, fieldNo, and entry as indexes.



Text File Information Table

Information from the input text file will be read into a table as well.

record	entry	field	value
record	entry	field	value
...			

Binary to Text

The PCT will use the text format table to determine which fields it needs to display. It will use the table to obtain the correct descriptions, fieldId, type, and length information. Then, all three numbers in the fieldId will be used to retrieve the actual binary data. PCT will check to make sure all the formats are correct and then print out the information to the text file.

Text to Binary

PCT will go through the text file information table and use the fieldId information to retrieve the offset and data information from the description table.

Appendix A ISDN Disconnection Causes

This source of this appendix is from ETS 300 102-1 Annex G. You can download the complete ETS 300 102-1 standard (ISDN layer 3 basic call control) from **WWW.ETSI.ORG** by searching the working documents from the site.

Normal class

1	Unallocated (unassigned) number
2	No route to specified transit network
3	No route to destination
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
26	Non-selected user clearing
27	Destination out of order
28	Invalid format (address incomplete)
29	Facility rejected
30	Response to status enquiry
31	Normal, unspecified

Resource Unavailable Class

34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
44	Request circuit/channel not available
47	Resource unavailable, unspecified

Service or option not available class

49	Quality of service not available
50	Requested facility not subscribed
57	Bearer capability not authorized

58	Bearer capability not presently available
63	Service or option not available, unspecified

Service or option not implemented class

65	Bearer capability not implemented
66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified

Invalid message (e.g. parameter out of range) class

81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identify does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
88	Incompatible destination
91	Invalid transit network selection
95	Invalid message, unspecified

Protocol error (e.g. unknown message) class

96	Mandatory information element is missing
97	Message type non-existent or not implemented
98	Message not compatible with call state or message type non-existent or not implemented
99	Information element non-existent or not implemented
100	Invalid information element contents
101	Message not compatible with call start
102	Recovery on timer expiry
111	Protocol error, unspecified

Interworking class

127	Interworking unspecified

Appendix B Error Code in Syslog

Use CI commond **'sys log disp i'** to see detail logs.
For example,

> sys log disp i
62 112 PP0a INTL call failed, rnp=576de0, code = -3022

This code –3022 means filter groups are mixed, so call is not allowed (call failed)

-3000	remote node is connecting
-3001	configured incoming call only, outgoing call fails
-3002	configured outgoing call only, incoming call fails
-3003	packet is filtered
-3004	no iface
-3005	no channel available
-3006	call request fail
-3007	remote node is waiting call back
-3020	call dial fail
-3022	filter groups are mixed, so call is not allowed
-3023	received unexpected event
-3024	state timeout
-3025	waiting RADIUS authentication
-3026	RADIUS call back fail
-3028	the node is not found
-3029	the node is inactive
-3030	dial fail
-3031	no budget
-3032	radius authentication fail
-3033	CLID is required
-3034	CLID can not be found
-3035	an outgoing call has already been placed for this remote node
-3036	call is blocked
-3037	invalid phone number
-3038	remote side is busy
-3039	no carrier
-3040	no dial tone
-3041	remote node is not active

-3042	no answer received
-3043	dial timeout
-3044	redial no method
-3045	redial stopped
-3046	redial no number
-3047	node is obtained but ppp is not up yet, second call has the same CLID
-3048	remote node does not supported L2TP

Appendix C PPP Numbers

POINT-TO-POINT PROTOCOL FIELD ASSIGNMENTS

PPP DLL PROTOCOL NUMBERS

The Point-to-Point Protocol (PPP) Data Link Layer [146,147,175] contains a 16 bit Protocol field to identify the encapsulated protocol. The Protocol field is consistent with the ISO 3309 (HDLC) extension mechanism for Address fields. All Protocols MUST be assigned such that the least significant bit of the most significant octet equals "0", and the least significant bit of the least significant octet equals "1".

Assigned PPP DLL Protocol Numbers

Value (in hex)	Protocol Name	
0001	Padding Protocol	
0003 to 001f	reserved (transparency inefficient)	
0021	Internet Protocol version 4	
0023	OSI Network Layer	
0025	Xerox NS IDP	
0027	DECnet Phase IV	
0029	AppleTalk	
002b	Novell IPX	
002d	Van Jacobson Compressed TCP/IP	
002f	Van Jacobson Uncompressed TCP/IP	
0031	Bridging PDU	
0033	Stream Protocol (ST-II)	
0035	Banyan Vines	
0037	reserved (until 1993)	
0039	AppleTalk EDDP	
003b	AppleTalk SmartBuffered	
003d	Multi-Link	[RFC1717]
003f	NETBIOS Framing	
0041	Cisco Systems	
0043	Ascom Timeplex	
0045	Fujitsu Link Backup and Load Balancing (LBLB)	
0047	DCA Remote Lan	
0049	Serial Data Transport Protocol (PPP-SDTP)	
004b	SNA over 802.2	
004d	SNA	
004f	IPv6 Header Compression	
0051	KNX Bridging Data	[ianp]
0053	Encryption	[Meyer]
0055	Individual Link Encryption	[Meyer]
0057	Internet Protocol version 6	[Hinden]
006f	Stampede Bridging	
0071	Reserved	[Fox]
0073	MP+ Protocol	[Smith]
007d	reserved (Control Escape)	[RFC1661]
007f	reserved (compression inefficient)	[RFC1662]
0081	Reserved Until 20-Oct-2000	[IANA]
0083	Reserved Until 20-Oct-2000	[IANA]
00c1	NTCITS IPI	[Ungar]
00cf	reserved (PPP NLPID)	
00fb	single link compression in multilink	[RFC1962]
00fd	compressed datagram	[RFC1962]
00ff	reserved (compression inefficient)	
02xx-1exx	(compression inefficient)	
0201	802.1d Hello Packets	
0203	IBM Source Routing BPDU	
0205	DEC LANBridge100 Spanning Tree	
0207	Cisco Discovery Protocol	[Sastry]

0209 Netcs Twin Routing [Korfmacher]
0231 Luxcom
0233 Sigma Network Systems
0235 Apple Client Server Protocol [Ridenour]
0281 Tag Switching - Unicast [Davie]
0283 Tag Switching - Multicast [Davie]

4001 Cray Communications Control Protocol [Stage]
4003 CDPD Mobile Network Registration Protocol [Quick]
4021 Stacker LZS [Simpson]
4023 RefTek Protocol [Banfill]

8001-801f Not Used - reserved [RFC1661]
8021 Internet Protocol Control Protocol
8023 OSI Network Layer Control Protocol
8025 Xerox NS IDP Control Protocol
8027 DECnet Phase IV Control Protocol
8029 Appletalk Control Protocol
802b Novell IPX Control Protocol
802d reserved
802f reserved
8031 Bridging NCP
8033 Stream Protocol Control Protocol
8035 Banyan Vines Control Protocol
8037 reserved till 1993
8039 reserved
803b reserved
803d Multi-Link Control Protocol
803f NETBIOS Framing Control Protocol
8041 Cisco Systems Control Protocol
8043 Ascom Timeplex
8045 Fujitsu LBLB Control Protocol
8047 DCA Remote Lan Network Control Protocol (RLNCP)
8049 Serial Data Control Protocol (PPP-SDCP)
804b SNA over 802.2 Control Protocol
804d SNA Control Protocol
804f IP6 Header Compression Control Protocol
8051 KNX Bridging Control Protocol [ianp]
8053 Encryption Control Protocol [Meyer]
8055 Individual Link Encryption Control Protocol [Meyer]
8057 IPv6 Control Protovol [Hinden]
806f Stampede Bridging Control Protocol
8073 MP+ Control Protocol [Smith]
8071 Reserved [Fox]
807d Not Used - reserved [RFC1661]
8081 Reserved Until 20-Oct-2000 [IANA]
8083 Reserved Until 20-Oct-2000 [IANA]
80c1 NTCITS IPI Control Protocol [Ungar]
80cf Not Used - reserved [RFC1661]
80fb single link compression in multilink control [RFC1962]
80fd Compression Control Protocol [RFC1962]
80ff Not Used - reserved [RFC1661]
8207 Cisco Discovery Protocol Control [Sastry]
8209 Netcs Twin Routing [Korfmacher]
8235 Apple Client Server Protocol Control [Ridenour]
8281 Tag Switching - Unicast [Davie]
8283 Tag Switching - Multicast [Davie]

c021 Link Control Protocol
c023 Password Authentication Protocol
c025 Link Quality Report
c027 Shiva Password Authentication Protocol
c029 CallBack Control Protocol (CBCP)
c02b BACP Bandwidth Allocation Control Protocol [RFC2125]
c02d BAP [RFC2125]
c081 Container Control Protocol [KEN]
c223 Challenge Handshake Authentication Protocol
c225 RSA Authentication Protocol [Narayana]
c227 Extensible Authentication Protocol [RFC2284]
c229 Mitsubishi Security Info Exch Ptcl (SIEP) [Seno]

c26f	Stampede Bridging Authorization Protocol	
c281	Proprietary Authentication Protocol	[KEN]
c283	Proprietary Authentication Protocol	[Tackabury]
c481	Proprietary Node ID Authentication Protocol	[KEN]

It is recommended that values in the "02xx" to "1exx" and "xx01" to "xx1f" ranges not be assigned, as they are compression inefficient.

Protocol field values in the "0xxx" to "3xxx" range identify the network-layer protocol of specific datagrams, and values in the "8xxx" to "bxxx" range identify datagrams belonging to the associated Network Control Protocol (NCP), if any.

Protocol field values in the "4xxx" to "7xxx" range are used for protocols with low volume traffic which have no associated NCP.

Protocol field values in the "cxxx" to "exxx" range identify datagrams as Control Protocols (such as LCP).

PPP LCP AND IPCP CODES

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP), the Compression Control Protocol (CCP), Internet Protocol Control Protocol (IPCP), and other control protocols, contain an 8 bit Code field which identifies the type of packet. These Codes are assigned as follows:

Code	Packet Type	
0	Vendor Specific	[RFC2153]
1	Configure-Request	
2	Configure-Ack	
3	Configure-Nak	
4	Configure-Reject	
5	Terminate-Request	
6	Terminate-Ack	
7	Code-Reject	
8	* Protocol-Reject	
9	* Echo-Request	
10	* Echo-Reply	
11	* Discard-Request	
12	* Identification	
13	* Time-Remaining	
14	+ Reset-Request	[RFC1962]
15	+ Reset-Reply	[RFC1962]

* LCP Only
+ CCP Only

PPP LCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) specifies a number of Configuration Options which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option	
0	Vendor Specific	[RFC2153]
1	Maximum-Receive-Unit	
2	Async-Control-Character-Map	
3	Authentication-Protocol	
4	Quality-Protocol	
5	Magic-Number	
6	DEPRECATED (Quality-Protocol)	
7	Protocol-Field-Compression	
8	Address-and-Control-Field-Compression	
9	FCS-Alternatives	[RFC1570]
10	Self-Describing-Pad	[RFC1570]
11	Numbered-Mode	[RFC1663]
12	DEPRECATED (Multi-Link-Procedure)	
13	Callback	[RFC1570]
14	DEPRECATED (Connect-Time)	
15	DEPRECATED (Compound-Frames)	
16	DEPRECATED (Nominal-Data-Encapsulation)	
17	Multilink-MRRU	[RFC1717]
18	Multilink-Short-Sequence-Number-Header	[RFC1717]

19	Multilink-Endpoint-Discriminator	[RFC1717]
20	Proprietary	[KEN]
21	DCE-Identifier	[SCHNEIDER]
22	Multi-Link-Plus-Procedure	[Smith]
23	Link Discriminator for BACP	[RFC2125]
24	LCP-Authentication-Option [	Culbert]
25	Consistent Overhead Byte Stuffing (COBS)	[Carlson]
26	Prefix elision	[Bormann]
27	Multilink header format	[Bormann]

IPV6CP CONFIGURATION OPTIONS

IPV6CP Configuration Options allow negotiation of desirable IPv6 parameters. IPV6CP uses the same Configuration Option format defined for LCP, with a separate set of Options. If a Configuration Option is not included in a Configure-Request packet, the default value for that Configuration Option is assumed.

1	Interface-Token	[RFC2023]
2	IPv6-Compression-Protocol	[RFC2023]

PPP ECP CONFIGURATION OPTION TYPES

A one octet field is used in the Encryption Control Protocol (ECP) to indicate the configuration option type [RFC1968].

ECP Option	Configuration Type	
0	OUI	[RFC1968]
1	Deprecated (DESE)	[Fox]
2	3DESE	[Kummert]
3	DESE-bis	[Fox]
4-255	Unassigned	

PPP CCP CONFIGURATION OPTION TYPES

A one octet field is used in the Compression Control Protocol (CCP) to indicate the configuration option type [RFC1962].

CCP Option	Configuration Type	
0	OUI	[RFC1962]
1	Predictor type 1	[RFC1962]
2	Predictor type 2	[RFC1962]
3	Puddle Jumper	[RFC1962]
4-15	unassigned	
16	Hewlett-Packard PPC	[RFC1962]
17	Stac Electronics LZS	[RFC1974]
18	Microsoft PPC	[RFC2118]
19	Gandalf FZA	[RFC1962]
20	V.42bis compression	[RFC1962]
21	BSD Compress	[RFC1977]
22	unassigned	
23	23 LZS-DCP	[RFC1967]
24	MVRCA (Magnalink)	[RFC1975]
25	DCE	[RFC1976]
26	Deflate	[RFC1979]
27-254	unassigned	
255	Reserved	[RFC1962]

The unassigned values 4-15 are intended to be assigned to other freely available compression algorithms that have no license fees.

PPP SDCP CONFIGURATION OPTIONS

A one octet field is used in the Compression Control Protocol (CCP) PPP Serial Data Transport Protocol (SDTP) to indicate the option type [RFC1963].

SDCP Option	Configuration Element	
1	Packet-Format	[RFC1963]
2	Header-Type	[RFC1963]
3	Length-Field-Present	[RFC1963]

4	Multi-Port	[RFC1963]
5	Transport-Mode	[RFC1963]
6	Maximum-Frame-Size	[RFC1963]
7	Allow-Odd-Frames	[RFC1963]
8	FCS-Type	[RFC1963]
9	Flow-Expiration-Time	[RFC1963]

Note that Option Types 5-8 are specific to a single port and require port numbers in their format. Option Types 6-8 are specific to the HDLC-Synchronous Transport-Mode.

PPP AUTHENTICATION ALGORITHMS

A one octet field is used in the Challenge-Handshake Authentication Protocol (CHAP) to indicate which algorithm is in use [RFC1994].

Number	Name	
0	Reserved	[RFC1994]
1	Reserved	[RFC1994]
2	Reserved	[RFC1994]
3	Reserved	[RFC1994]
4	Reserved	[RFC1994]
5	CHAP with MD5	[RFC1994]
128	MS-CHAP	[Crocker]

PPP LCP FCS-ALTERNATIVES

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) FCS-Alternatives Configuration Option contains an 8-bit Options field which identifies the FCS used. These are assigned as follows:

Bit	FCS
1	Null FCS
2	CCITT 16-Bit FCS
4	CCITT 32-bit FCS

PPP MULTILINK ENDPOINT DISCRIMINATOR CLASS

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) Multilink Endpoint Discriminator Option includes a Class field which identifies the address class, These are assigned as follows:

Class	Description	
0	Null Class	[RFC1717]
1	Locally Assigned	[RFC1717]
2	Internet Protocol (IPv4)	[RFC1717]
3	IEEE 802.1 global MAC address	[RFC1717]
4	PPP Magic Number Block	[RFC1717]
5	Public Switched Network Director Number	[RFC1717]

PPP LCP CALLBACK OPERATION FIELDS

The Point-to-Point Protocol (PPP) Link Control Protocol (LCP) Callback Configuration Option contains an 8-bit Operations field which identifies the format of the Message. These are assigned as follows:

Operation	Description
0	Location determined by user authentication.
1	Dialing string.
2	Location identifier.
3	E.164 number.
4	X.500 distinguished name.
5	unassigned
6	Location is determined during CBCP negotiation.

PPP IPCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Internet Protocol Control Protocol (IPCP) specifies a number of Configuration Options which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option	
1	IP-Addresses (deprecated)	[RFC1332]
2	IP-Compression-Protocol	[RFC1332]
3	IP-Address	[RFC1332]
4	Mobile-IPv4	[RFC2290]
129	Primary DNS Server Address	[RFC1877]
130	Primary NBNS Server Address	[RFC1877]
131	Secondary DNS Server Address	[RFC1877]
132	Secondary NBNS Server Address	[RFC1877]

PPP ATCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Apple Talk Control Protocol (ATCP) specifies a number of Configuration Options [RFC-1378] which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	AppleTalk-Address
2	Routing-Protocol
3	Suppress-Broadcasts
4	AT-Compression-Protocol
5	Reserved
6	Server-information
7	Zone-information
8	Default-Router-Address

PPP OSINLCP CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) OSI Network Layer Control Protocol (OSINLCP) specifies a number of Configuration Options [RFC1377] which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	Align-NPDU

PPP BANYAN VINES CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Banyan Vines Control Protocol (BVCP) specifies a number of Configuration Options [RFC1763] which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	BV-NS-RTP-Link-Type
2	BV-FRP
3	BV-RTP
4	BV-Suppress-Broadcast

PPP BRIDGING CONFIGURATION OPTION TYPES

The Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP) specifies a number of Configuration Options which are distinguished by an 8 bit Type field. These Types are assigned as follows:

Type	Configuration Option
1	Bridge-Identification
2	Line-Identification
3	MAC-Support
4	Tinygram-Compression
5	LAN-Identification
6	MAC-Address
7	Spanning-Tree-Protocol

PPP BRIDGING MAC TYPES

The Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP) contains an 8 bit MAC Type field which identifies the MAC encapsulated. These Types are assigned as follows:

Type	MAC	
0	Reserved	
1	IEEE 802.3/Ethernet	with cannonical addresses
2	IEEE 802.4	with cannonical addresses
3	IEEE 802.5	with non-cannonical addresses
4	FDDI	with non-cannonical addresses
5-10	reserved	
11	IEEE 802.5	with cannonical addresses
12	FDDI	with cannonical addresses

PPP BRIDGING SPANNING TREE

The Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP) Spanning Tree Configuration Option contains an 8-bit Protocol field which identifies the spanning tree used. These are assigned as follows:

Protocol	Spanning Tree
0	Null - no spanning tree protocol supported
1	IEEE 802.1D spanning tree protocol
2	IEEE 802.1G extended spanning tree protocol
3	IBM source route spanning tree protocol
4	DEC LANbridge 100 spanning tree protocol

PPP INTERNETWORK PACKET EXCHANGE CONTROL PROTOCOL (IPXCP)

IPXCP CONFIGURATION OPTIONS

Option	Description	Reference
1	IPX-Network-Number	[RFC1552]
2	IPX-Node-Number	[RFC1552]
3	IPX-Compression-Protocol	[RFC1552]
4	IPX-Routing-Protocol	[RFC1552]
5	IPX-Router-Name	[RFC1552]
6	IPX-Configuration-Complete	[RFC1552]

IPX COMPRESSION PROTOCOL VALUES

Value	Protocol	Reference
2	Telebit Compressed IPX	[Fox]
235	Shiva Compressed NCP/IPX	[Fox]

IPX-ROUTING-PROTOCOL OPTIONS

Value	Protocol	Reference
0	No routing protocol required	[RFC1552]
1	RESERVED	[RFC1552]
2	Novell RIP/SAP required	[RFC1552]
4	Novell NLSP required	[RFC1552]
5	Novell Demand RIP required	[RFC1582]
6	Novell Demand SAP required	[RFC1582]
7	Novell Triggered RIP required	[Edmonstone]
8	Novell Triggered SAP required	[Edmonstone]

NBFCP Configuration Options

NBFCP Configuration Options [RFC 2097] allow modifications to the standard characteristics of the network-layer protocol to be negotiated. If a Configuration Option is not included in a Configure-Request packet, the default value for that Configuration Option is assumed.

NBFCP uses the same Configuration Option format defined for LCP, with a separate set of Options.

Current values are assigned as follows:

1 Name-Projection
2 Peer-Information
3 Multicast-Filtering
4 IEEE-MAC-Address-Required

PPP EAP REQUEST/RESPONSE TYPES

A one octet field is used in the Extensible Authentication Protocol (EAP) to indicate the function and structure of EAP Request and Response packets [RFC2284].

Type	Description	
1	Identity	[RFC2284]
2	Notification	[RFC2284]
3	Nak (Response only)	[RFC2284]
4	MD5-Challenge	[RFC2284]
5	One Time Password (OTP)	[RFC2289]
6	Generic Token Card	[RFC2284]
7		
8		
9	RSA Public Key Authentication	[Whelan]
10	DSS Unilateral	[Nace]
11	KEA	[Nace]
12	KEA-VALIDATE	[Nace]
13	EAP-TLS	[Adoba]
14	Defender Token (AXENT)	[Rosselli]

PPP VENDOR SPECIFIC OUI OPTIONS

There are some provisions in some PPP message formats for vendor specific options to be identified by the Organisationally Unique Identifier (OUI), namely the first three octets of a Vendor's Ethernet address assigned by IEEE 802 [RFC1968. RFC2153]. These are listed in the "ethernet-numbers" file (see http://www.iana.org/in-notes/iana/assignments/ethernet-numbers).

Appendix D Cable Pinouts

This appendix provides the following pinout information:

Console Port Signals and Pinouts

Your router comes with a console cable that you need to connect a console terminal (an VT100 terminal or PC running terminal emulation software) to your router. Different router comes with different console cable. The console cable includes:

- RJ45-to-DB25 cable
- DB9-to-DB25 cable
- RJ45-to-Mac-Mini-Din-8 cable
- DB9-to-Mac-Mini-Din-8 cable

Table D-1: RJ45-to-DB25 Console Cabling Signal and Pinouts

RJ45 Plug	DB-25 pin	Console Device Signal
1	6	DSR
2	20	DTR
3	2	TXD
4	4	RTS
5	7	Signal Ground
6	3	RXD
7	5	CTS
8	8	DCD
SHIELD	SHIELD	SHIELD

Table D-2: DB9-to-DB25 Console Cabling Signal and Pinouts

DB-9 pin	DB-25 pin	Console Device Signal
1	8	DSR
2	3	RXD
3	2	TXD
4	20	DTR
5	7	Signal Ground
6	6	DSR+
7	4	RTS

8	5	CTS
9	22	DSR-
SHIELD	SHIELD	SHIELD

Table D-3: RJ45-to-Mac-Mini-Din-8 cable

RJ45 Plug	MINI DIN 8	Console Device Signal
1		
2	1	RTS
3	3	TXD
4	1	RTS
5	4,8	GND
6	5	RXD
7	2	CTS
8	7	CD
SHIELD	SHIELD	SHIELD

Table D-4: DB9-to-Mac-Mini-Din-8 cable

RJ45 Plug	MINI DIN 8	Console Device Signal
1	7	CD
2	5	RXD
3	3	TXD
4	1	RTS
5	4,8	GND
6	6	NC
7	1	RTS
8	2	CTS
9		
SHIELD	SHIELD	SHIELD

Ethernet Cable Signals and Pinouts

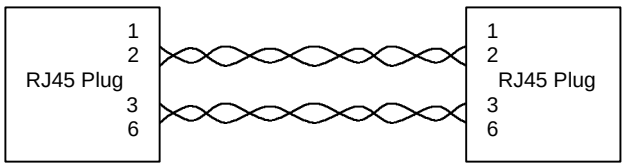
Straight Cable & Crossover Cable

Straight Cable

The Prestige router comes with two LAN cables, one is RJ45-to-RJ45 straight cable with white tag, and the other is crossover RJ45-to-RJ45 cable with red tag. Use the straight RJ45-to-RJ45 cable to connect a PC to the 4-port HUB of Prestige. Table D-2 lists the pinouts for the straight RJ45-to-RJ45 cable.

Table D-5: Straight RJ45-to-RJ45 cable pinouts

RJ45	Signal	RJ45
1	TD+	1
2	TD-	2



3	RD+	3
4	Not used by 10BaseT	4
5	Not used by 10BaseT	5
6	RD-	6
7	Not used by 10BaseT	7
8	Not used by 10BaseT	8

Crossover Cable

A crossover cable reverses the transmit and receive pairs at the two ends of the RJ45 connectors. When linking the Prestige HUB router to another HUB you need the crossover RJ45-to-RJ45 cable. Figure D-1 shows how to connect the Prestige HUB router to a HUB and a PC. Table D-6 lists the pinouts for the crossover RJ45-to-RJ45 cable.

Table D-6: Crossover RJ45-to-RJ45 cable pinouts

RJ45	Signal	RJ45
1	TD+	3
2	TD-	6
3	RD+	1
4	Not used by 10BaseT	4
5	Not used by 10BaseT	5
6	RD-	2
7	Not used by 10BaseT	7
8	Not used by 10BaseT	8

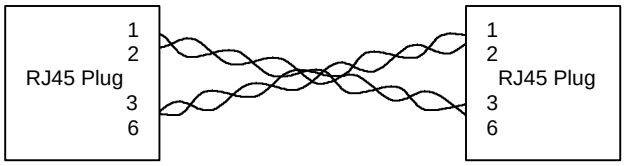
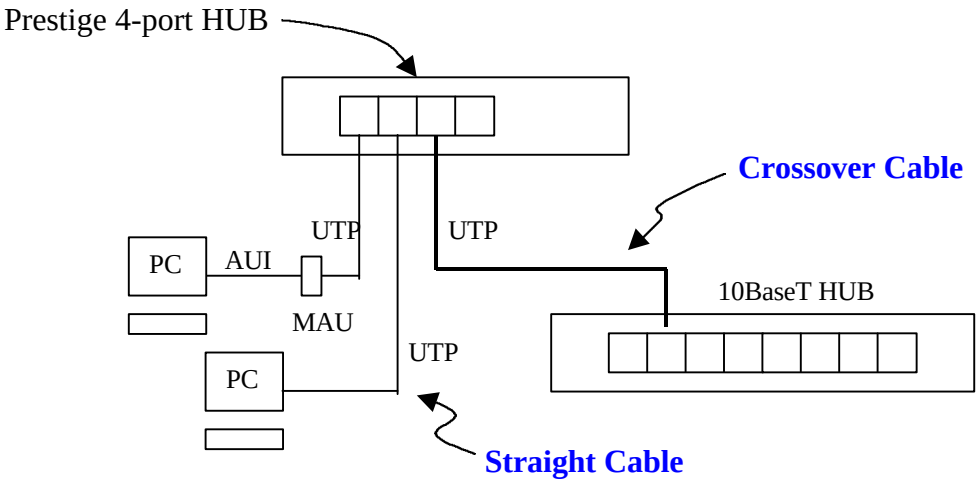


Figure D-1



ISDN BRI Port Pinouts

Table D-7 lists the ISDN BRI port pinouts.

Table D-7: BRI Port (RJ-45) Pinouts

RJ-45	TE	NT	Polarity
3	Transmit	Receive	+
4	Receive	Transmit	+
5	Receive	Transmit	-
6	Transmit	Receive	-

* Pins 1, 2, 7, and 8 are not used.
* TE refers to terminal terminating layer 1 aspects of TE1, TA, and NT2 functional groups.
* NT refers to network terminating layer 1 aspects of NT1 and NT2 functional groups.

Appendix E Frequently Used CI Commands

Here is the brief description about the most frequently used CI commands. The sequence of the following table is based on the commands' alphabetic order.

CI Command	brief description
bridge stat disp	statistics on Bridge packets
bridge blt disp	Bridge LAN table
bridge brt disp	Bridge WAN table
dev channel disp [bri0 | bri1]	show channel information on bri0 or bri1
dev channel drop [bri0 | bri1]	drop channel bri0 or bri1
dev dial x	manually dial to remote node x; x is the remote node number here
ether config	show the current Ethernet configuration
ether driver cnt disp	statistics on the Ethernet driver
Exit	exit from CI mode
ip address	LAN IP address
ip ping {IP address}	Ping {IP address}
ip route stat	IP routing table
ip status	statistics on IP packets
ip sua iface [wanif0 | wanif1] disp	display the SUA table for iface wanif0 or wanif1
ipx route stat	IPX routing table
ipx sap stat	IPX SAP table
isdn atring clear [bri0 | bri1]	clear the ISDN ring buffer of bri0 or bri1
isdn atring disp [bri0 | bri1]	display the ISDN ring buffer of bri0 or bri1
isdn config	show the current ISDN configuration
isdn fw ana dump	display ISDN trace messages on screen
isdn fw ana [on | off]	enable/disable ISDN trace mechanism
Isdn fw cnt disp	display ISDN transmission counters
isdn initstring clear	clear ISDN init string
isdn initstring set {at commands}	set ISDN init string to {at commands}
isdn reset	initialize the ISDN line
ppp lcp acfc [on | off]	enable/disable PPP LCP ACFC negotiation
ppp lcp bacp [on | off]	enable/disable PPP LCP BACP negotiation
ppp lcp callback [on | off]	enable/disable PPP LCP Microsoft callback negotiation
ppp lcp pfc [on | off]	enable/disable PPP LCP PFC negotiation
sys countrycode x	set country code
sys trcl call	show call trace on the screen
sys log disp	display the error/warning/information messages in the system log
sys log clear	clear the existing contents in system log
sys mbuf pool	display the pool of mbuf; mbuf is the buffer pre-allocated for data transmission
sys mbuf status	display mbuf status
sys memutil mqueue	statistics on pre-allocated system memory cell
sys memutil usage	statistics on the memory utilization
sys stdio 0	set SMT session timeout value to 0 –> never timeout
sys trcd	display the packet trace on screen
sys trcl clear	clear the existing contents in logic trace log
sys trcl disp	display the contents in both of logic and packet trace logs
sys trcl switch [on|off]	enable/disable logic trace log mechanism
sys trcp chann [in|out|both|enet0]	Enable the packet trace mechanism on incoming, outgoing, or

	both from WAN; or from Ethernet.
sys trcp disp	display the contents in packet trace log
sys trcp switch [on|off]	enable/disable packet trace log mechanism