P-660 series

Support Notes

(For P-660R-61/63/67-C)

Version3.40
Sep. 2005

ZyXEL
Unleash Networking Power

INDEX

ZyNOS FAQ

1. What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all Prestige routers that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites as they become available.

2. How do I access the Prestige SMT menu?

The SMT interface is a menu driven interface, 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 with 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 the SMT access.

3. What is the default console port baud rate? Moreover, how do I change it?

The default console port baud rate is 9600bps. When configuring the SMT, please make sure the terminal baud rate is also 9600bps. You can change the console baud rate from 9600bps to 115200bps in SMT menu 24.2.2.

4. How do I update the firmware and configuration file?

You can upload the firmware and configuration file to Prestige using console port, FTP or TFTP client software. You CAN NOT upload the firmware and configuration file via Telnet because the Telnet connection will be dropped during uploading the firmware. Please do not power off the router right after the FTP or TFTP uploading is finished, the router will upload the firmware to its flash at this moment.

5. How do I upload the ZyNOS firmware code via console?

The procedure for uploading ZyNOS via console is as follows.

a. Enter debug mode when powering on the Prestige using a terminal emulator
b. Enter 'ATUR' to start the uploading

c. Use X-modem protocol to transfer the ZyNOS code
d. Enter 'ATGO' to restart the Prestige

6. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN?

The Prestige allows you to transfer the firmware to Prestige by using TFTP program via LAN. The procedure for uploading ZyNOS via TFTP is as follows.

a. Use the TELNET client program in your PC to login to your Prestige.
b. Enter CI command **'sys stdio 0'** in menu 24.8 to disable console idle timeout
c. To upgrade firmware, use TFTP client program to put firmware in file **'ras'** in the Prestige. After data transfer is finished, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.
d. To backup your firmware, use the TFTP client program to get file **'ras'** from the Prestige.

7. How do I upload ROMFILE via console port?

In some situations, you may need to upload the ROMFILE, such as losing the system password, or the need of resetting SMT to factory default.

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

a. Enter debug mode when powering on the Prestige using a terminal emulator
b. Enter **'ATLC'** to start the uploading
c. Use X-modem protocol to transfer ROMFILE
d. Enter **'ATGO'** to restart the Prestige

8. How do I restore SMT configurations by using TFTP client program via LAN?

a. Use the TELNET client program in your PC to login to your Prestige.
b. Enter CI command **'sys stdio 0'** in menu 24.8 to disable console idle timeout.
c. To backup the SMT configurations, use TFTP client program to get file **'rom-0'** from the Prestige.
d. To restore the SMT configurations, use the TFTP client program to put your configuration in file **rom-0** in the Prestige.

9. What should I do if I forget the system password?

In case you forget the system password, you can erase the current configuration and restore factory defaults in three way.

a. Use the Web Configurator.

b. Use the **RESET button** on the rear panel of P-660 to reset the router. After the router is reset, the LAN IP address and the SMT password will be reset to **'192.168.1.1'** and **'1234'**. So now you can reach the router through console port or telnet again.
c. Upload the default ROMFILE via console port to reset the SMT to factory default. After uploading ROMFILE, the default system password is **'1234'**.

10. How to use the Reset button?

a. Turn your Prestige off and then on. Make sure the **SYS** led is on (not blinking)
b. Press the **RESET** button for five seconds and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the Prestige restarts.

11.What is SUA? When should I use SUA?

SUA (Single User Account) is a unique feature supported by Prestige router which allows multiple people to access Internet concurrently for the cost of a single user account.

When Prestige acting as SUA receives a packet from a local client destined for the outside Internet, it replaces the source address in the IP packet header with its own address and the source port in the TCP or UDP header with another value chosen out of a local pool. It then recomputes the appropriate header checksums and forwards the packet to the Internet as if it is originated from Prestige using the IP address assigned by ISP. When reply packets from the external Internet are received by Prestige, the original IP source address and TCP/UDP source port numbers are written into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to its true destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

12. What is the difference between SUA and Multi-NAT?

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. The P-660 now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple severs of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions that supported SUA 'visible' servers had to be of different types. The P-660 supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The P-660 supports 8 sets since there are 8 remote node. The default SUA (Read Only) Set in menu 15.1.255 is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions.

13. Is it possible to access a server running behind SUA from the outside Internet? If possible, how?

Yes, it is possible because P-660 delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured in Menu 15.2.1 - **NAT Server Setup**.

14. When do I need Multi-NAT?

- Make local server accessible from outside Internet

When NAT is enabled the local computers are not accessible from outside. You can use Multi-NAT to make an internal server accessible from outside.

- Support Non-NAT Friendly Applications

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. Thus, users on the same network can not login to the same server simultaneously. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user login to the server using a unique global IP address.

15. What IP/Port mapping does Multi-NAT support?

NAT supports five types of IP/port mapping. They are: One to One, Many to One, Many to Many Overload, Many to Many No Overload and Server. The details of the mapping between ILA and IGA are described as below. Here we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA),

1. **One to One**

In One-to-One mode, the P-660 maps one ILA to one IGA.

2. **Many to One**

In Many-to-One mode, the P-660 maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

3. **Many to Many Overload**

In Many-to-Many Overload mode, the P-660 maps the multiple ILA to shared IGA.

4. **Many One-to-One**

In Many One-to-One mode, the P-660 maps each ILA to unique IGA.

5. **Server**

In Server mode, the P-660 maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note, if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1

Many-to-One (SUA/PAT)	ILA1<--->IGA1
	ILA2<--->IGA1
	...

Many-to-Many Overload	ILA1<--->IGA1
	ILA2<--->IGA2
	ILA3<--->IGA1
	ILA4<--->IGA2
	...

Many
One-to-One
	ILA1<--->IGA1
	ILA2<--->IGA2
	ILA3<--->IGA3
	ILA4<--->IGA4
	...

Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

16. How many network users can the SUA/NAT support?

The Prestige does not limit the number of the users but the number of the sessions. The P-660 supports 1024/2048 sessions that you can use the **'ip nat iface wanif0 st'** command in menu 24.8 to view the current active sessions.

17. What are Device filters and Protocol filters?

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

18. Why can't I configure device filters or protocol filters?

In ZyNOS, you can not mix different filter groups in the same filter set.

19. How can I protect against IP spoofing attacks?

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

For the input data filter:

- Deny packets from the outside that claim to be from the inside
- Allow everything that is not spoofing us

Filter rule setup:

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

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

For the output data filters:

- Deny bounceback packet
- Allow packets that originate from us

Filter rule setup:

- Filter Type =TCP/IP Filter Rule
- Active =Yes
- Destination IP Addr =a.b.c.d
- Destination IP Mask =w.x.y.z
- Action Matched =Drop
- Action No Matched =Forward

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

General FAQ

1. How can I manage P-660?

- Menu driven user interface for easy network management Local and remote console management
- Web configurator
- Telnet remote management
- TFTP (Trivial File Transfer Protocol) and FTP firmware upgrade and configuration backup and restore

2. What is the default user name and password to loging web configurator?

The default user name is **'admin'** and password is **'1234'**. You can change the password when login to web configurator in the Advanced Setup->Password menu. **Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.**

3. How do I know the P-660's WAN IP address assigned by the ISP?

You can view **"My WAN IP <from ISP> : 200.1.1.1"** shown in menu 24.1 to check this IP address.

4. What is the micro filter or splitter used for?

Generally, the voice band uses the lower frequency ranging from 0 to 4KHz, while ADSL data transmission uses the higher frequency. The micro filter acts as a low-pass filter for your telephone set to ensure that ADSL transmissions do not interfere with your voice transmissions. For the details about how to connect the micro filter please refer to the user's manual.

5. The P-660 supports Bridge and Router mode, what's the difference between them ?

When the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use bridge mode which works as an ADSL modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to add another Internet sharing device, like a router. In this case, we use the router mode which works as a general Router plus an ADSL Modem.

6. How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the P-660 if the ISP uses PPPoE.

7. Why does my provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

8. What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as http://www.dyndns.org/.

Without DDNS, we always tell the users to use the WAN IP of the P-660 to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-660.

When the ISP assigns the P-660 a new IP, the P-660 updates this IP to DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

9. When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the P-660 sends this IP to the DDNS server for its updates.

10. What is DDNS wildcard? Does the P-660 support DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the hostname, *.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

Yes, the P-660 supports DDNS wildcard that http://www.dyndns.org/ supports. When using wildcard, you simply enter yourhost.dyndns.org in the Host field in Menu 1.1 Configure Dynamic DNS.

11. Can the P-660's SUA handle IPSec packets sent by the IPSec gateway?

Yes, the P-660's SUA can handle IPSec ESP Tunneling mode. We know when packets go through SUA, SUA will change the source IP address and source port for the host. To pass IPSec packets, SUA must understand the ESP packet with protocol number 50, replace the source IP address of the IPSec gateway to the router's WAN IP address. However, SUA should not change the source port of the UDP packets which are used for key managements. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

12. How do I setup my P-660 for routing IPSec packets over SUA?

For outgoing IPSec tunnels, no extra setting is required.

For forwarding the inbound IPSec ESP tunnel, A 'Default' server set in menu 15.2.1 is required. It is because SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP of this server in Menu 15. Thus SUA is able to forward the incoming packets to the requested service behind SUA and the outside users access the server using the P-660's WAN IP address. So, we have to configure the internal IPsec as a default server (unspecified service port) in menu 15.2.1 when it acts a server gateway.

13. What is Traffic Shaping?

Traffic Shaping is a feature in the P-660. It allocates the bandwidth to WAN dynamically and aims at boosting the efficiency of the bandwidth. If there are serveral VCs in the P-660 but only one VC activated at one time, the P-660 allocates all the Bandwidth to the VC and the VC gets full bandwidth. If another VCs are avtivated later, the bandwidth is yield to other VCs after ward.

14. What do the parameters (PCR, SCR, MBS) mean?

Traffic shaping parameters (PCR, SCR, MBS) can be set in Menu 4 and Menu 11.6 and is valid for both incoming and outgoing direction since G.shdsl is symmetric.
Peak Cell Rate(PCR): The maximum bandwidth allocated to this connection. The VC connection throughput is limited by PCR.
Sustainable Cell Rate(SCR): The least guaranteed bandwidth of a VC. When there are multi-VCs on the same line, the VC throughput is guaranteed by SCR.
Maximum Burst Size(MBS): The amount of cells transmitted through this VC at the Peak Cell Rate before yielding to other VCs. Total bandwidth of the line is dedicated to single VC if there is only one VC on the line. However, as the other VC asking the bandwidth, the MBS defines the maximum number of cells transmitted via this VC with Peak Cell rate before yielding to other VCs.

The P-660 holds the parameters for shaping the traffic among its virtual channels. If you do not need traffic shaping, please set SCR = 0, MBS = 0 and PCR as the maximum value according to the line rate (for example, 2.3 Mbps line rate will result PCR as 5424 cell/sec.)

15.Why do we perform traffic shaping in the P-660 ?

The P-660 must manage traffic fairly and provide bandwidth allocation for different sorts of applications, such as voice, video, and data. All applications have their own natural bit rate. Large data transactions have a fluctuating natural bit rate. The P-660 is able to support variable traffic among different virtual connections. Certain traffic may be discarded if the virtual connection experiences congestion. Traffic shaping defines a set of actions taken by the P-660 to avoid congestion; traffic shaping takes measures to adapt to unpredictable fluctuations in traffic flows and other problems among virtual connections.

ADSL FAQ

1. **How does ADSL compare to Cable modems?**

ADSL provides a dedicated service over a single telephone line; cable modems offer a dedicated service over a shared media. While cable modems have greater downstream bandwidth capabilities (up to 30 Mbps), that bandwidth is shared among all users on a line, and will therefore vary, perhaps dramatically, as more users in a neighborhood get online at the same time. Cable modem upstream traffic will in many cases be slower than ADSL, either because the particular cable modem is inherently slower, or because of rate reductions caused by contention for upstream bandwidth slots. The big difference between ADSL and cable modems, however, is the number of lines available to each. There are no more than 12 million homes passed today that can support two-way cable modem transmissions, and while the figure also grows steadily, it will not catch up with telephone lines for many years. Additionally, many of the older cable networks are not capable of offering a return channel; consequently, such networks will need significant upgrading before they can offer high bandwidth services.

2. What is the expected throughput?

In our test, we can get about 1.6Mbps data rate on 15Kft using the 26AWG loop. The shorter the loop, the better the throughput. Besides, please do not stay in menu 24.1 it will slow down the throughput.

3. What is the micro filter used for?

Generally, the voice band uses the lower frequency ranging from 0 to 4KHz, while ADSL data transmission uses the higher frequency. The micro filter acts as a low-pass filter for your telephone set to ensure that ADSL transmissions do not interfere with your voice transmissions. For the details about how to connect the micro filter please refer to the user's manual.

4. How do I know the ADSL line is up?

You can see the DSL LED on the P-660's front panel is on when the ADSL physical layer is up.

5. How does the P-660 work on a noisy ADSL?

Depending on the line quality, the P-660 uses "Fall Back" and "Fall Forward" to automatically adjust the date rate.

6. Does the VC-based multiplexing perform better than the LLC-based multiplexing?

Though the LLC-based multiplexing can carry multiple protocols over a single VC, it requires extra header information to identify the protocol being carried on the virtual circuit (VC). The VC-based multiplexing needs a separate VC for carrying each protocol but it does not need the extra headers. Therefore, the VC-based multiplexing is more efficient.

7. How do I know the details of my ADSL line statistics?

You can use the following CI commands to check the ADSL line statistics.

```
CI> wan adsl perfdata
CI> wan adsl status
CI> sys log disp
CI> wan adsl linedata far
CI> wan adsl linedata near
```

8.What are the possible reasons when the ADSL link is down?

The physical ADSL line may not be up if:

(1) The DSLAM is not Alcatel.
(2) If it is Alcatel, the firmware version should be above 3.1.

9.What are the signaling pins of the ADSL connector?

The signaling pins on the P-660's ADSL connector are pin 3 and pin 4. The middle two pins for a RJ11 cable.

General Application Notes

1. Internet Access Using P-660 under Bridge mode

- Setup your workstation
- Setup your P-660 under bridge mode

If the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use P-660 which works as an ADSL bridge modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet. See the figure below for this setup.

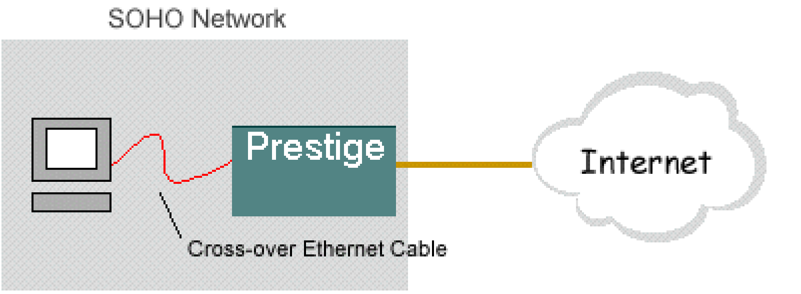


Figure: Internet Access Using Modem Mode

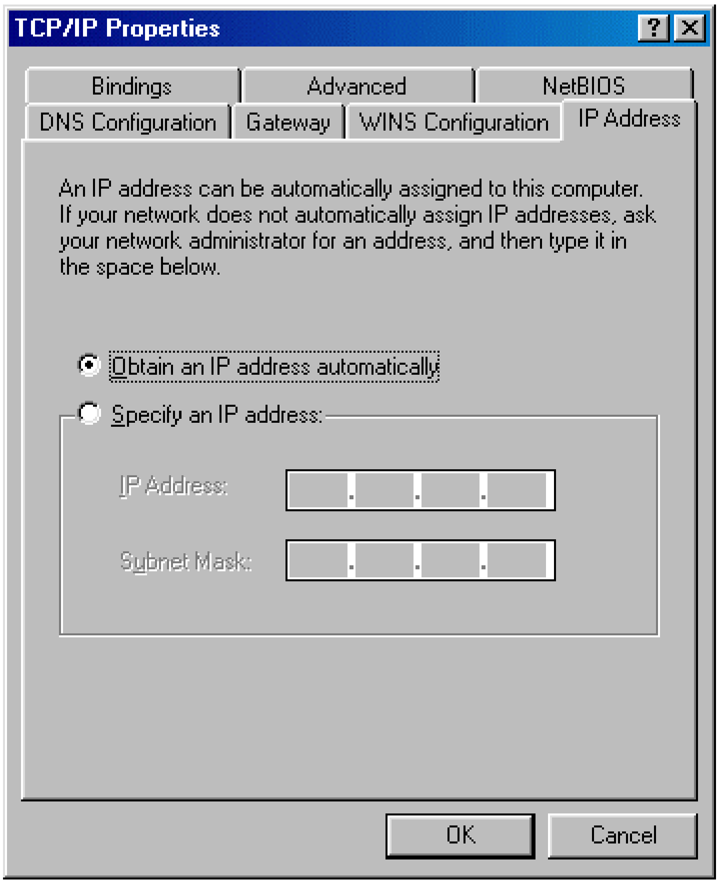
Set up your workstation

1. Ethernet connection

To connect your computer to the P-660's LAN port, the computer must have an Ethernet adapter card installed. For connecting a single computer to the P-660, we use a ***cross-over*** Ethernet cable.

2. TCP/IP configuration

In most cases, the IP address of the computer is assigned by the ISP dynamically so you have to configure the computer as a DHCP client which obtains the IP from the ISP using DHCP protocol. The ISP may also provide the gateway, DNS via DHCP if they are available. Otherwise, please enter the static IP addresses for all that the ISP gives to you in the network TCP/IP settings. For Windows, we check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup, please see the example shown below.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

Setup your P-660 under bridge mode

The following procedure shows you how to configure your P-660 as an ADSL Modem for bridging traffic. We will use SMT menu to guide you through the related menu. You can use console or Telnet for finishing these configurations.

1. Configure P-660 as bridge mode in Menu 1 General Setup.

```
  Menu 1 － General setup

System name=P-660
Location=
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No
Route IP= No
Bridge= Yes
```

2. Configure a LAN IP for the P-660 and turn off DHCP Server in Menu 3.2-TCP/IP Ethernet Setup. We use 192.168.1.1 in this case.

```
Menu 3.2 - TCP/IP and DHCP 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
      Remote DHCP Server= N/A
   TCP/IP Setup:
      IP Address= 192.168.1.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= None
        Version= N/A
      Multicast= None
      IP Policies=
      Edit IP Alias= No
```

3. Configure for Internet setup in Menu 11-Remote Node Profile.

```
  Menu 11.1 - Remote Node Profile

         Rem Node Name= Bridge        Route= None
         Active= Yes                  Bridge= Yes
         Encapsulation= RFC 1483      Edit IP/Bridge= No
         Multiplexing= LLC-based      Edit ATM Options= No
         Service Name= N/A            Edit Advance Options= No
         Incoming:                           Telco Option:
           Rem Login= N/A             Allocated Budget(min)= N/A
           Rem Password= N/A          Period(hr)= N/A
         Outgoing:                     Schedule Sets= N/A
           My Login= N/A               Nailed-Up Connection= N/A
           My Password= N/A             Session Options:
           Authen= N/A                 Edit Filter Sets= No
                                       Idle Timeout(sec)= N/A
```

Key Settings:

Option	**Description**
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
Router/ Bridge	Disable routing mode and enable bridge mode, Bridge = Yes.

4. Configure ATM setting in Menu 11.6-Remote Node ATM Layer Options. In Menu 11.1, setup "Edit ATM Options= Yes" to enter Menu 11.6 sub-Menu.

```
Menu 11.6 - Remote Node ATM Layer Options

     VPI #= 0
     VCI #= 33
     ATM QoS Type= CBR
     Peak Cell Rate (PCR)= 0
     Sustain Cell Rate (SCR)= 0
     Maximum Burst Size (MBS)= 0
```

Key Settings:

Option	Description
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.

2. Internet Access Using P-660 under Router mode

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to install an Internet sharing device, like a router. In this case, we use the P-660 which works as a general Router plus an ADSL Modem. See the figure below for this setup.

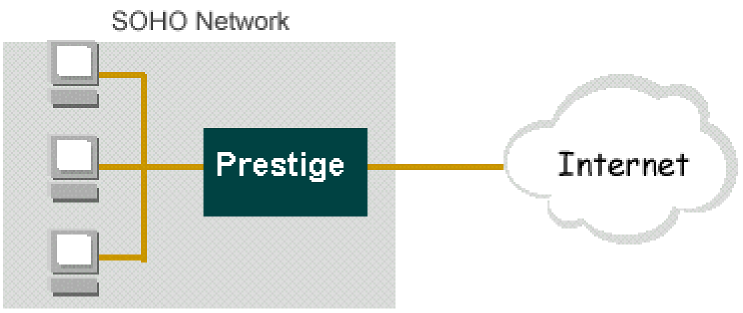


Figure: Internet Access Using P652

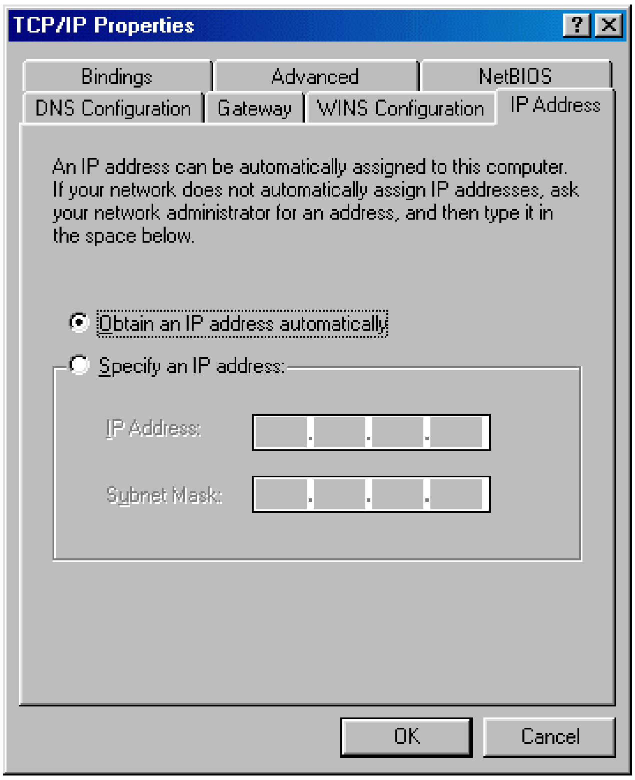
Set up your workstation

1. Ethernet connection

Connect the LAN ports of all computers and the P-660 to a HUB using a straight Ethernet cable.

2. TCP/IP configuration

Since the P-660 is set to DHCP server as default, so you need only to configure the workstations as the DHCP clients in the networking settings. In this case, the IP address of the computer is assigned by the P-660. The P-660 can also provide the DNS to the clients via DHCP if it is available. For this setup in Windows, we check the option '***Obtain an IP address automatically***' in its TCP/IP setup. Please see the example shown below.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address:

Subnet Mask:

Set up your P-660

The following procedure shows you how to configure your P-660 as Router mode for routing traffic. We will use SMT menu to guide you through the related menu. You can use console or Telnet for finishing these configurations.

1. Configure P-660 as router mode in Menu 1 General Setup.

```
                              Menu 1– General Setup

                              System Name= P-660
                              Location=
Contact Person's Name=
  Domain Name=
   Edit Dynamic DNS= No
  Route IP= Yes
   Bridge= No
```

2. Configure a LAN IP for the P-660 and the DHCP settings in Menu 3.2-TCP/IP Ethernet Setup. The settings except of the DNS addresses shown below are the pre-configured defaults.

```
Menu 3.2 - TCP/IP and DHCP Setup
DHCP Setup
          DHCP= Server
          Client IP Pool Starting Address= 192.168.1.33
          Size of Client IP Pool= 6
          Primary DNS Server= 168.95.1.1
          Secondary DNS Server= 168.95.192.1
          Remote DHCP Server= N/A
TCP/IP Setup:
          IP Address= 192.168.1.1
          IP Subnet Mask= 255.255.255.0
          RIP Direction= Both
          Version= RIP-1
          Multicast= None
          IP Policies=
          Edit IP Alias= No
```

3. Configure for Internet setup in Menu 4-Internet Access Setup.

```
             Menu 4 - Internet Access Setup

          ISP's Name= CHT
          Encapsulation= PPPoE
          Multiplexing= LLC-based
          VPI #= 0
          VCI #= 33
          ATM QoS Type= CBR
             Peak Cell Rate (PCR)= 0
             Sustain Cell Rate (SCR)= 0
             Maximum Burst Size (MBS)= 0
          My Login= cso@hinet.net
```

```
            My Password= ********
            Idle Timeout (sec)= 0
            IP Address Assignment= Dynamic
              IP Address= N/A
            Network Address Translation= SUA Only
              Address Mapping Set= N/A

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

Key Settings:

Option	**Description**
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.
Single User Account	Set to **Yes** if you only have a single IP account for sharing with local computers.
IP Address Assignment	Set to **Dynamic** if the ISP provides the IP for the P-660 dynamically. Otherwise, set to **Static** and enter the IP in the following **IP Address** field.
IP Address	This field can not be configured if the ISP provides the IP for the P-660 dynamically. Otherwise, enter the IP that the ISP gives to you.

3. Setup the P-660 as a DHCP Relay

What is DHCP Relay?

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P-660 supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the LAN clients. When it is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 1.

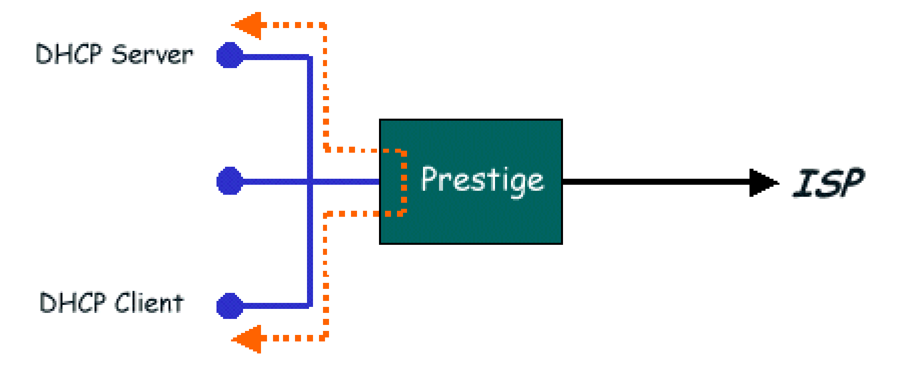


Figure1: Prestige as a DHCP Relay

Setup the P-660 as a DHCP Client

1. Toggle the DHCP to Relay in menu 3.2 and enter the IP address of the DHCP server in the **'Relay Server Address'** field.

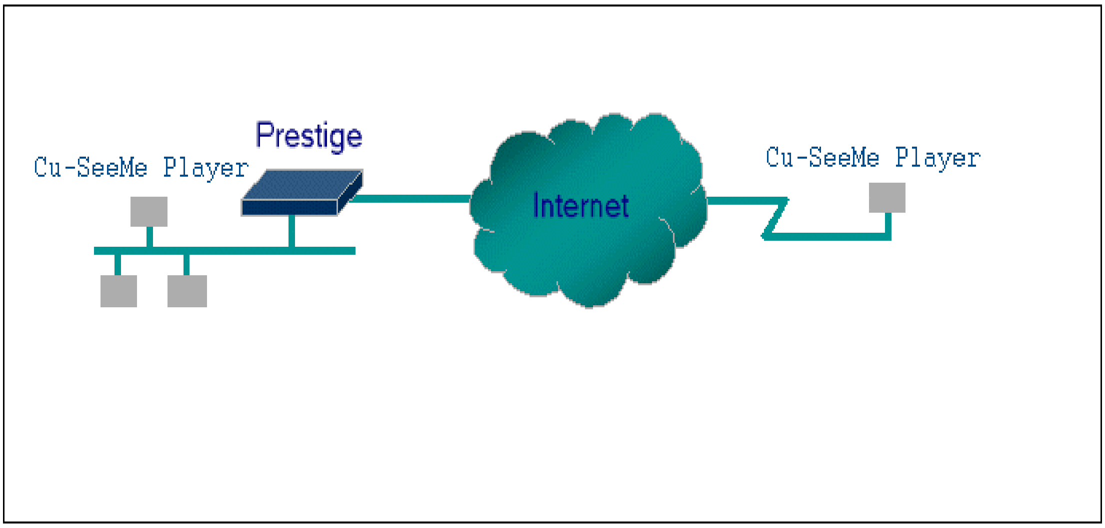
```
                    Menu 3.2 - TCP/IP and DHCP Ethernet Setup

          DHCP Setup
           DHCP= Relay
           Client IP Pool Starting Address= N/A
           Size of Client IP Pool= N/A
           Primary DNS Server= N/A
           Secondary DNS Server= N/A
           Relay Server Address= 192.168.1.2

          TCP/IP Setup:
           IP Address= 192.168.1.1
           IP Subnet Mask= 255.255.255.0
           RIP Direction= Both
             Version= RIP-1
           Multicast= None
           IP Policies=
           Edit IP Alias= No
           Press ENTER to Confirm or ESC to Cancel:
```

4. SUA Notes

Tested SUA/NAT Applications (e.g., Cu-SeeMe, ICQ, NetMeeting)



Introduction

Generally, SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. However, some applications such as Cu-SeeMe, and ICQ will need to connect to the local user behind the P-660. In such case, a SUA server must be entered in menu 15.2.1 to forward the incoming packets to the true destination behind SUA. Generally, we do not need extra settings of menu 15.2.1 for an outgoing connection. But for some applications we need to configure the menu 15.2.1 to make the outgoing connection work. After the required menu 15.2.1 settings are completed the internal server or client applications can be accessed by using the P-660's ***WAN IP*** address.

SUA Supporting Table

The following are the required menu 15.2.1 settings for the various applications running SUA mode.

ZyXEL SUA Supporting Table[1]

Application	Required Settings in Menu 15.2.1 Port/IP	
	Outgoing Connection	Incoming Connection
HTTP	None	80/client IP
FTP	None	21/client IP
TELNET	None	23/client IP (and remove Telnet filter in WAN port)
POP3	None	110/client IP
SMTP	None	25/client IP
mIRC	None for Chat. For DCC, please set Default/Client IP	

Windows PPTP	None	1723/client IP
ICQ 99a	None for Chat. For DCC, please set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
ICQ 2000b	None for Chat	None for Chat
ICQ Phone 2000b	None	6701/client IP
Cornell 1.1 Cu-SeeMe	None	7648/client IP
White Pine 3.1.2 Cu-SeeMe[2]	7648/client IP & 24032/client IP	Default/client IP
White Pine 4.0 Cu-SeeMe	7648/client IP & 24032/client IP	Default/client IP
Microsoft NetMeeting 2.1 & 3.01[3]	None	1720/client IP 1503/client IP
Cisco IP/TV 2.0.0	None	
RealPlayer G2	None	
VDOLive	None	
Quake1.06[4]	None	Default/client IP
QuakeII2.30[5]	None	Default/client IP
QuakeIII1.05 beta	None	
StartCraft	6112/client IP	
Quick Time 4.0	None	
pcAnywhere 8.0	None	5631/client IP 5632/client IP 22/client IP
IPsec (ESP tunneling mode)	None (one client only)	Default/Client
Microsoft Messenger Service 3.0	6901/client IP	6901/client IP
Microsoft Messenger Service 4.6/ 4.7/ 5.0 (none UPnP)[6]	None for Chat, File transfer ,Video and Voice	None for Chat, File transfer, Video and Voice
Net2Phone	None	6701/client IP
Network Time Protocol (NTP)	None	123 /server IP
Win2k Terminal Server	None	3389/server IP
Remote Anything	None	3996 - 4000/client IP

Virtual Network Computing (VNC)	None	5500/client IP 5800/client IP 5900/client IP
AIM (AOL Instant Messenger)	None for Chat and IM	None for Chat and IM
e-Donkey	None	4661 - 4662/client IP
POLYCOM Video Conferencing	None	Default/client IP
iVISTA 4.1	None	80/server IP
Microsoft Xbox Live[7]	None	N/A

[1] Since SUA enables your LAN to appear as a single computer to the Internet, it is not possible to configure similar servers on the same LAN behind SUA.

[2] Because White Pine Cu-SeeMe uses dedicate ports (port 7648 & port 24032) to transmit and receive data, therefore only one local Cu-SeeMe is allowed within the same LAN.

[3] In SUA mode, only one local NetMeeting user is allowed because the outsiders can not distinguish between local users using the same internet IP.

[4] Certain Quake servers do not allow multiple users to login using the same unique IP, so only one Quake user will be allowed in this case. Moreover, when a Quake server is configured behind SUA, P-660 will not be able to provide information of that server on the internet.

[5] Quake II has the same limitations as that of Quake I.

[6] P-660 support MSN Messenger 4.6/ 4.7/ 5.0 video/ voice pass-through NAT since new firmware version. In addition, for the Windows OS supported UPnP (Universal Plug and Play), such as Windows XP and Windows ME, UPnP supported in P-660 is an alternative solution to pass through MSN Messenger video/ voice traffic. For more detail, please refer to UPnP application note.

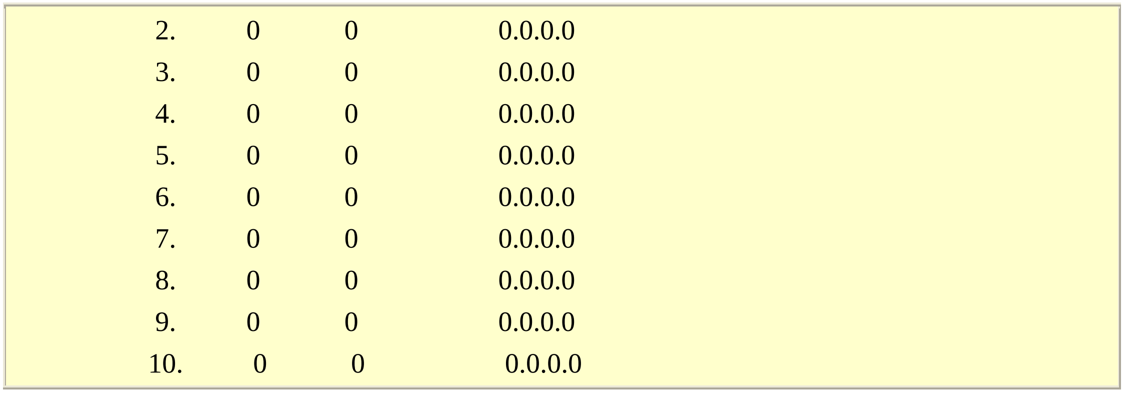
[7] P-660 support Microsoft Xbox Live since the new firmware version. If your P-660 firmware is too old to support such function, you may have a work-around solution, please refer to ZyXEL website -> Support -> Xbox Live service http://www.zyxel.com/support/xbox.htm

Configurations

For example, if the workstation operating Cu-SeeMe has an IP of 192.168.1.34, then the default SUA server must be set to 192.168.1.34. The peer Cu-SeeMe user can reach this workstation by using P-660's ***WAN IP*** address which can be obtained from menu 24.1.

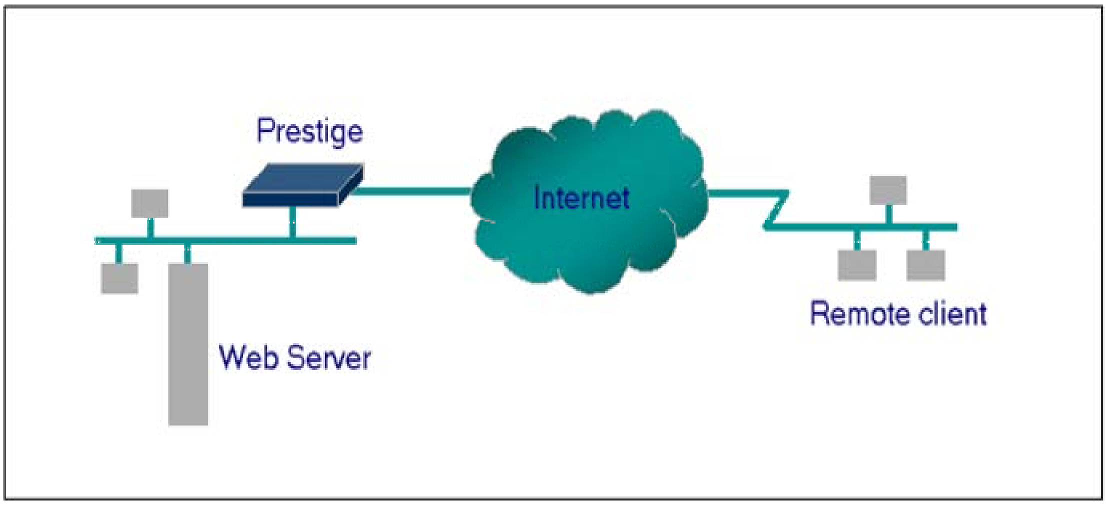
```
     Menu 15.2.1 - NAT Server Setup (Used for SUA Only)


    Rule Start Port No. End Port No. IP Address
   -------------------------------------------------
     1.     Default      Default      192.168.1.34
```



```
          2.      0       0            0.0.0.0
          3.      0       0            0.0.0.0
          4.      0       0            0.0.0.0
          5.      0       0            0.0.0.0
          6.      0       0            0.0.0.0
          7.      0       0            0.0.0.0
          8.      0       0            0.0.0.0
          9.      0       0            0.0.0.0
         10.       0       0            0.0.0.0
```

Configure 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 P-660, 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 request 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 15.2.1', Multiple Server Configuration.

The outside users can access the local server using the P-660's ***WAN IP*** address which can be obtained from menu 24.1.

For example (Configuring an internal Web server for outside access) :

```
          Menu 15.2.1 - NAT Server Setup (Used for SUA Only)


        Rule Start Port No. End Port No. IP Address
       ---------------------------------------------------
         1.     Default      Default      0.0.0.0
         2.       80           80        192.168.1.10
         3.        0            0        0.0.0.0
         4.        0            0        0.0.0.0
         5.        0            0        0.0.0.0
         6.        0            0        0.0.0.0
         7.        0            0        0.0.0.0
         8.        0            0        0.0.0.0
         9.        0            0        0.0.0.0
        10.        0            0       0.0.0.0
        11.        0            0       0.0.0.0
        12.        0            0       0.0.0.0

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

Port numbers for some services

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

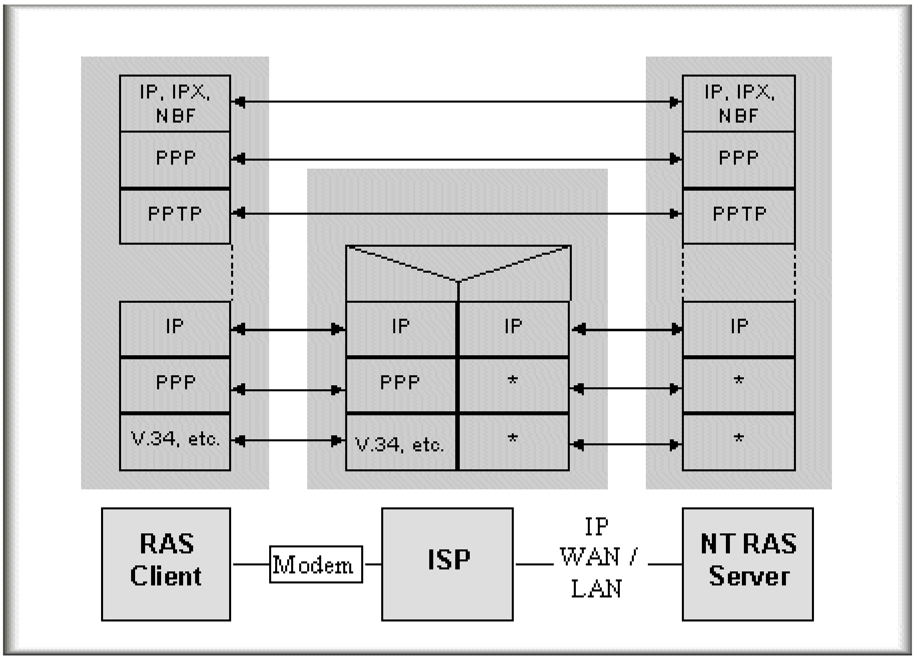
Configure a PPTP server behind SUA

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 Windows 9x 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 dial-up 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.



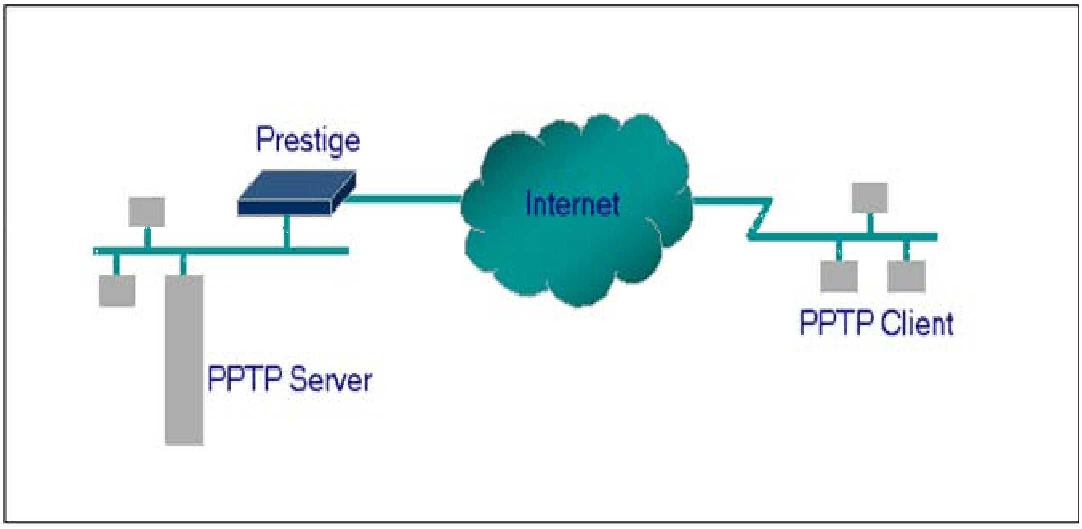
Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

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 with a remote private network in the P-660 SUA case. In ZyNOS, all PPTP packets can be forwarded to the internal PPTP Server (WinNT server) behind SUA. The port number of the PPTP has to be entered in the SMT Menu 15 for P-660 to forward to the appropriate private IP address of Windows NT server.



Example

The following example shows how to dial to an ISP via the P-660 and then establish 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 the P-660.

1. 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 NetBEUI
- Set the Internet gateway to P-660

2. PPTP client setup (Win9x)

- Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the P-660's Internet IP address for logging to NT RAS server.
- Set the Internet gateway to the router that is connecting to ISP

3. P-660 router setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect P-660 router to your ISP first.
- Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown below.

```
           Menu 15.2.1 - NAT Server Setup (Used for SUA Only)



        Rule Start Port No. End Port No. IP Address
       --------------------------------------------------
         1.     Default      Default      0.0.0.0
         2.       1723        1723        192.168.1.10
         3.        0           0         0.0.0.0
         4.        0           0         0.0.0.0
         5.        0           0         0.0.0.0
         6.        0           0         0.0.0.0
         7.        0           0         0.0.0.0
         8.        0           0         0.0.0.0
         9.        0           0         0.0.0.0
        10.        0           0         0.0.0.0
        11.        0           0         0.0.0.0
        12.        0           0         0.0.0.0

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

When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the Internet. If the Internet connection between two LANs is achievable, you can place a VPN call from the remote Win9x client.

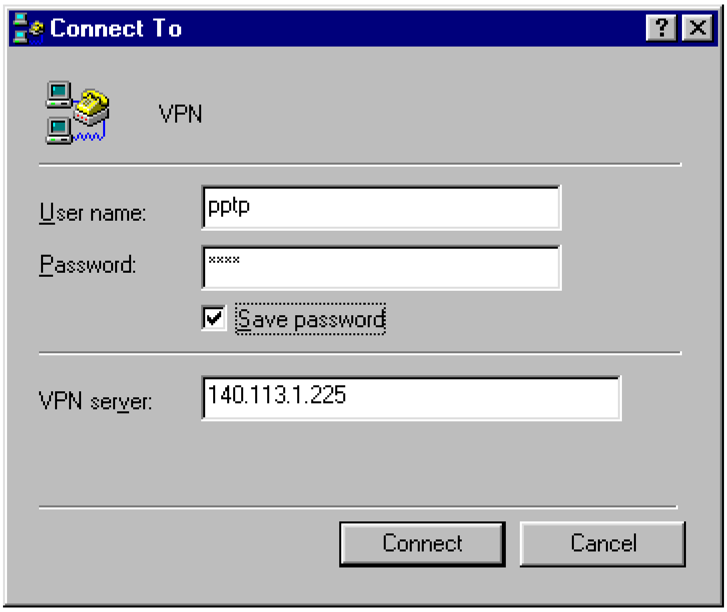
For example: C:\ping 203.66.113.2

When a dial-up connection to ISP is established, a default gateway is assigned to the router traffic through that connection. Therefore, the output below shows the default gateway of the Win9x client after the dial-up connection has been established.

Before making a VPN connection from the Win9x client to the NT server, you need to know the exact Internet IP address that the ISP assigns to P-660 router in SUA mode and enter this IP address in the VPN dial-up dialog box. You can check this Internet

IP address from PNC Monitor or 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 by ISP. 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.



User name: pptp

Password: ****

☑ Save password

VPN server: 140.113.1.225

5. Using Multi-NAT

What is Multi-NAT?

NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the P-660, thus preventing intruders from probing your network.

The SUA feature that the P-660 supports previously operates by mapping the private IP addresses to a global IP address. It is only one subset of the NAT. The P-660 with ZyNOS V3.40 supports the most of the features of the NAT based on RFC 1631, and we call this feature as **'Multi-NAT'**. For more information on IP address translation, please refer to RFC 1631, ***The IP Network Address Translator (NAT)*.**

How NAT works

If we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA), see the following figure. The term 'inside' refers to the set of networks that are subject to translation. NAT operates by mapping the ILA to the IGA required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers) and then forwards each packet to the Internet ISP, thus making them appear as if they had come from the NAT system itself (e.g., the P-660 router). The P-660 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

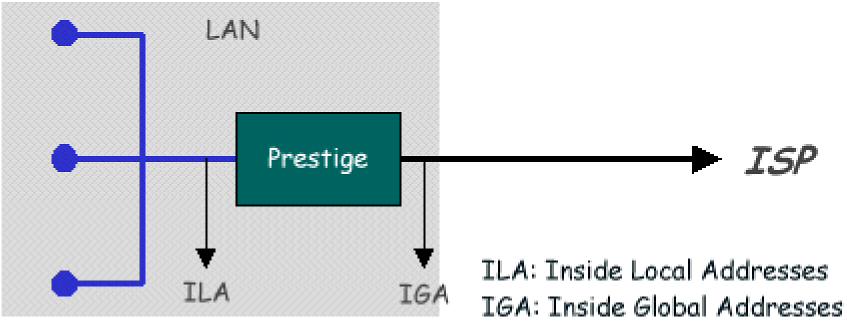


Figure1: Local/Global IP Addresses

NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

One to One

In One-to-One mode, the P-660 maps one ILA to one IGA.

Many to One

In Many-to-One mode, the P-660 maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

Many to Many Overload

In Many-to-Many Overload mode, the P-660 maps the multiple ILA to shared IGA.

Many to Many No Overload

In Many-to-Many No Overload mode, the P-660 maps each ILA to unique IGA.

Server

In Server mode, the P-660 maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note, if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes these types.

NAT Type	**IP Mapping**	**Mapping Direction**
One-to-One	ILA1<--->IGA1	Both
Many-to-One (SUA/PAT)	ILA1---->IGA1 ILA2---->IGA1 ...	Outgoing
Many-to-Many Overload	ILA1---->IGA1 ILA2---->IGA2 ILA3---->IGA1 ILA4---->IGA2 ...	Outgoing
Many-to-Many No Overload (Allocate by Connections)	ILA1---->IGA1 ILA2---->IGA3 ILA3---->IGA2 ILA4---->IGA4 ...	Outgoing
Server	Server 1 IP<----IGA1 Server 2 IP<----IGA1	Incoming

SUA Versus NAT

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. The P-660 now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple severs of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions (that supported SUA 'visible' servers had to be of different types. The P-660 supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The P-660 supports 8 sets since there are 8 remote node. The default SUA (Read Only) Set in menu 15.1 is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions.

SMT Menus

Applying NAT in the SMT Menus

You apply NAT via menus 4 and 11.3 as displayed next. The next figure how you apply NAT for Internet access in menu 4. Enter 4 from the Main Menu to go to Menu 4-**Internet Access Setup**.

```
              Menu 4 - Internet Access Setup
          ISP's Name= CHT
          Encapsulation= PPPoE
          Multiplexing= LLC-based
          VPI #= 0
          VCI #= 33
          ATM QoS Type= CBR
             Peak Cell Rate (PCR)= 0
             Sustain Cell Rate (SCR)= 0
             Maximum Burst Size (MBS)= 0
          My Login= cso@hinet.net
          My Password= ********
          Idle Timeout (sec)= 0
          IP Address Assignment= Static
          IP Address= 200.1.2.1
          Network Address Translation= Full Feature
          Address Mapping Set= 1
      Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.3.

```
          Menu 11.3 - Remote Node Network Layer Options

     IP Options: Bridge Options:
     IP Address Assignment = Dynamic
```

```
                    Rem IP Addr = 0.0.0.0
                    Rem Subnet Mask= 0.0.0.0
                    My WAN Addr= N/A
                    NAT= Full Feature
                    Address Mapping Set= 1
                    Metric= 2
                    Private= No
                    RIP Direction= None
                      Version= RIP-1
                    Multicast= None
                    IP Policies=



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

Step 1. Enter 11 from the Main Menu.
Step 2. Move the cursor to the Edit IP field, press the [SPACEBAR] to toggle the default **No** to **Yes**, then press [ENTER] to bring up Menu 11.3-**Remote Node Network Layer Options**.

The following table describes the options for Network Address Translation.

Field	**Options**	**Description**
Network Address Translation	**Full Feature**	When you select this option the SMT will use Address Mapping Set 1 (Menu 15.1-see later for further discussion).
	None	NAT is disabled when you select this option.
	SUA Only	When you select this option the SMT will use Address Mapping Set 255 (Menu 15.1-see later for further discussion). This option use basically Many-to-One Overload mapping. Select **Full Feature** when you require other mapping types. It is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions. Note that there is also a **Server** type whose IGA is **0.0.0.0** in this set.

Table: Applying NAT in Menu 4 and Menu 11.3

Configuring NAT

To configure NAT, enter 15 from the Main Menu to bring up the following screen.

```
                    Menu 15 - NAT Setup

                 1. Address Mapping Sets
                 2. NAT Server Sets
```

Address Mapping Sets and NAT Server Sets

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to LAN clients. Each remote node must specify which NAT Address Mapping Set to use. The P-660 has 8 remote nodes and so allows you to configure 8 NAT Address Mapping Set. You can see nine NAT Address Mapping sets in Menu 15.1. You can only configure from Set 1 to Set 8. Set 255 is used for SUA. When you select **Full Feature** in menu 4 or 11.3, you must enter correct NAT Set as well. When you select **SUA Only**, the SMT will use Set 255.

The NAT Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the P-660), a server rule must be set up inside the NAT Address Mapping set. Please see NAT Server Sets for further information on these menus.

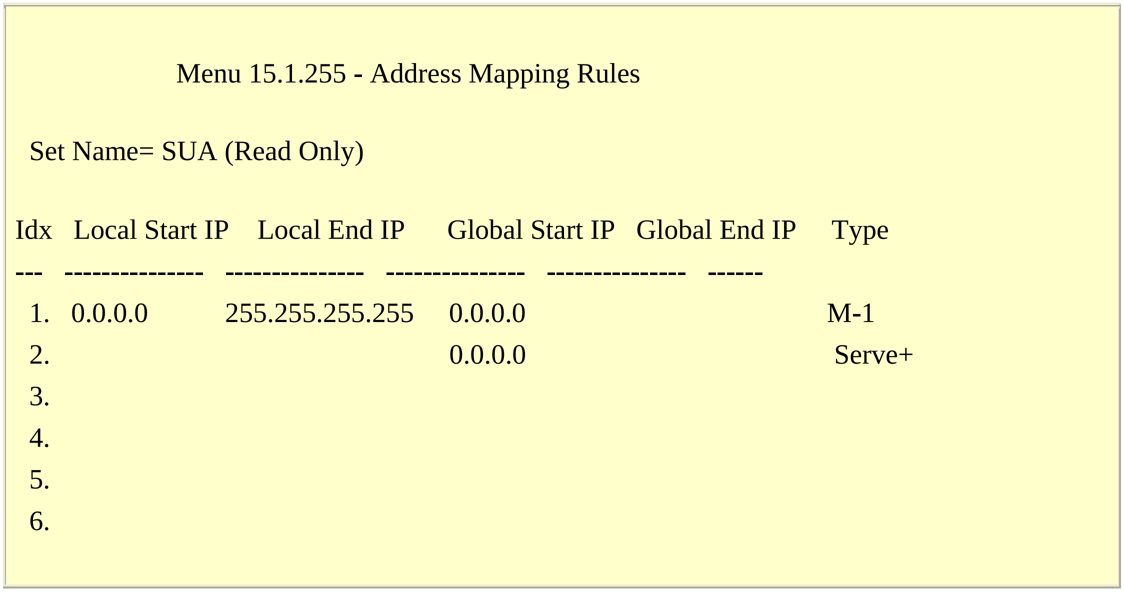
Enter 1 to bring up Menu 15.1-Address Mapping Sets

```
             Menu 15.1 - Address Mapping Sets

              1.
              2.
              3.
              4.
              5.
              6.
              7.
              8.
             255. SUA (Read Only)


                Enter Set Number to Edit:
```

Let's first look at Option 255. Option 255 is equivalent to SUA in previous ZyXEL routers. The fields in this menu cannot be changed. Entering 255 brings up this screen.



```
              Menu 15.1.255 - Address Mapping Rules

  Set Name= SUA (Read Only)

 Idx   Local Start IP    Local End IP     Global Start IP   Global End IP     Type
 ---   ---------------   ---------------   ---------------   ---------------   ------
   1.  0.0.0.0          255.255.255.255    0.0.0.0                             M-1
   2.                                      0.0.0.0                              Serve+
   3.
   4.
   5.
   6.
```

The following table explains the fields in this screen. Please note that the fields in this menu are read-only.

Field	Description	Option/Example
Set Name	This is the name of the set you selected in Menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	This is the starting local IP address (ILA).	0.0.0.0 for the Many-to-One type.
Local End IP	This is the starting local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	N/A
Type	This is the NAT mapping types.	Many-to-One and Server

Please note that the fields in this menu are read-only. However, the settings of the server set 1 can be modified in menu 15.2.1.

Now let's look at Option 1 in Menu 15.1. Enter 1 to bring up this menu.

```
              Menu 15.1.1 - Address Mapping Rules
Set Name= ?
Idx   Local Start IP    Local End IP     Global Start IP   Global End IP     Type
---   ---------------   ---------------   ---------------   ---------------   ------
  1.
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
  10.
             Action= Edit          , Select Rule= 0

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

We will just look at the differences from the previous menu. Note that, this screen is not read only, so we have extra Action and Select Rule fields. Not also that the [?] in the Set Name field means that this is a required field and you must enter a name for the set. The description of the other fields is as described above. The Type, Local and Global Start/End IPs are configured in Menu 15.1.1 (described later) and the values are displayed here.

Field	Description	Option
Set Name	Enter a name for this set of rules. This is a required field. **Please note that if this field is left blank, the entire set will be deleted.**	Rule1
Action	They are 4 actions. The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a new rule before the rule selected. The rule after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **Save Set** means to save the whole set (note when you choose this action the Select Rule item will be disabled).	Edit Insert Before Delete Save Set
Select Rule	When you choose **Edit**, **Insert Before** or **Save Set** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

Note: **Save Se**t in the **Action** field means to save the whole set. You must do this if you make any changes to the set-including deleting a rule. No changes to the set take place until this action is taken. Be careful when ordering your rules as each rule is executed in turn beginning from the first rule.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1-Address Mapping Rule** in which you can edit an individual rule and configure the Type, Local and Global Start/End IPs displayed in Menu 15.1.1.

```
  Menu 15.1.1.1 -   - Rule 1
Type: One-to-One
Local IP:
  Start= 0.0.0.0
  End   = N/A
Global IP:
  Start= 0.0.0.0
  End   = N/A
Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Field		Description	Option/Example
Type		Press [SPACEBAR] to toggle through a total of 5 types. These are the mapping types discussed above plus a server type. Some examples follow to clarify these a little more.	One-to-One Many-to-One Many-to-Many Overload Many-to-Many No Overload Server
Local IP	Start	This is the starting local IP address (ILA)	0.0.0.0
	End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for **One-to-One** type.	255.255.255.255
Global IP	Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
	End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** types.	200.1.1.64

Note: For all Local and Global IPs, the End IP address must begin after the IP Start address, i.e., you cannot have an End IP address beginning before the Start IP address.

NAT Server Sets

The NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu of before). If you wish, you can make inside servers for different services, e.g., Web or FTP, visible to the outside users, even though NAT makes your network appears as a single machine to the outside world. A server is identified by the port number, e.g., Web service is on port 80 and FTP on port 21.

As an example (see the following figure), if you have a Web server at 192.168.1.36 and a FTP server at 192.168.1.33, then you need to specify for port 80 (Web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.

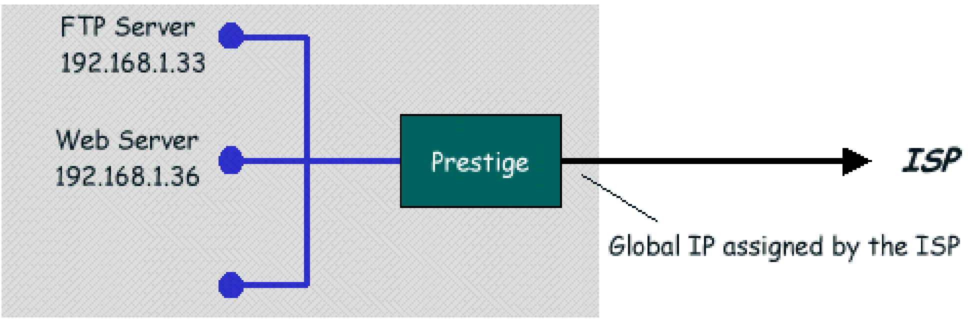


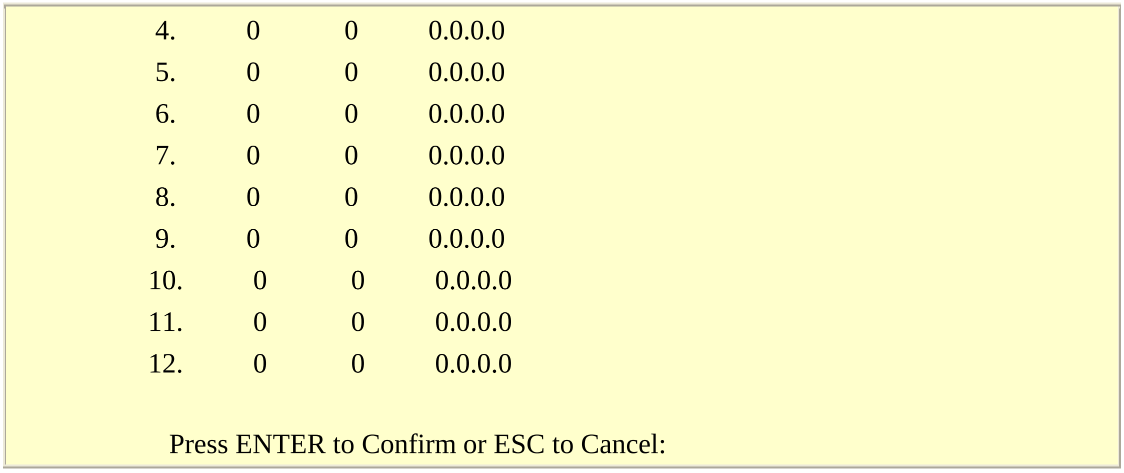
Figure: Configure Multiple Servers behind NAT

Please note that a server can support more than one service, e.g., a server can provide both FTP and Mail service, while another provides only Web service.

The following procedures show how to configure a server behind NAT.

Step 1. Enter 15 in the Main Menu to go to **Menu 15-NAT Setup**.
Step 2. Enter 2 to go to **Menu 15.2.1-NAT Server Setup**.
Step 3. Enter the service port number in the **Port#** field and the inside IP address of the server in the **IP Address** field.
Step 4. Press [SPACEBAR] at the 'Press ENTER to confirm...' prompt to save your configuration after you define all the servers or press ESC at any time to cancel.

```
  Menu 15.2.1 - NAT Server Setup (Used for SUA Only)
 Rule Start Port No. End Port No. IP Address
------------------------------------------------
  1.     Default      Default      0.0.0.0
  2.      21           21          192.168.1.33
  3.      80           80          192.168.1.36
```



```
          4.       0         0       0.0.0.0
          5.       0         0       0.0.0.0
          6.       0         0       0.0.0.0
          7.       0         0       0.0.0.0
          8.       0         0       0.0.0.0
          9.       0         0       0.0.0.0
         10.       0         0       0.0.0.0
         11.       0         0       0.0.0.0
         12.       0         0       0.0.0.0

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

The most often used port numbers are shown in the following table. Please refer RFC 1700 for further information about port numbers.

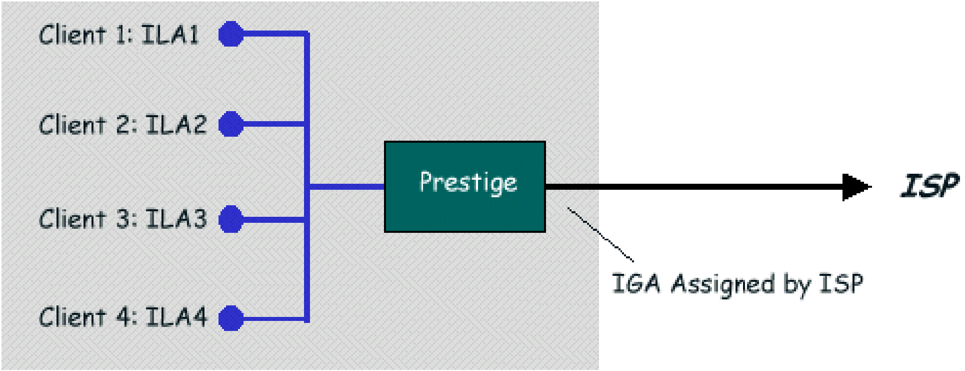
Service	**Port Number**
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

Examples

- Internet Access Only
- Internet Access with an Internal Server
- Using Multiple Global IP addresses for clients and servers
- Support Non NAT Friendly Applications

1. Internet Access Only

In our Internet Access example, we only need one rule where all our ILAs map to one IGA assigned by the ISP. See the following figure.



Internet Access Using NAT Many-to-One Mapping

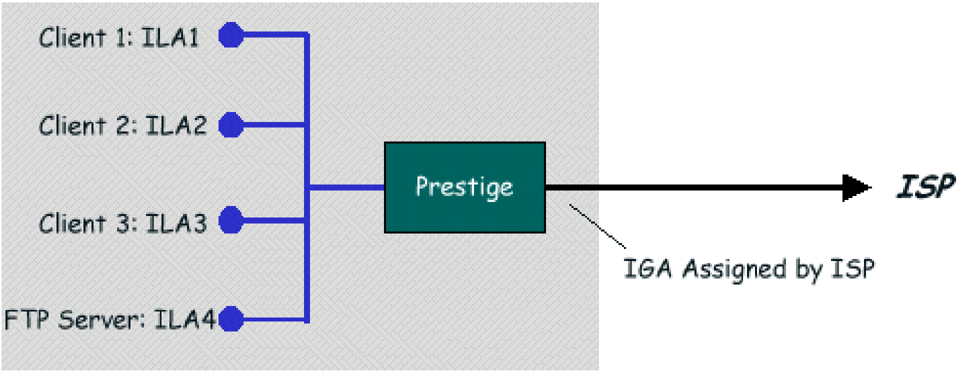
```
                Menu 4 - Internet Access Setup

               ISP's Name= CHT
               Encapsulation= PPPoE
               Multiplexing= LLC-based
               VPI #= 0
               VCI #= 33
               ATM QoS Type= CBR
                  Peak Cell Rate (PCR)= 0
                  Sustain Cell Rate (SCR)= 0
                  Maximum Burst Size (MBS)= 0
               My Login= cso@hinet.net
               My Password= ********
               Idle Timeout (sec)= 0
               IP Address Assignment= Dynamic
               IP Address= N/A
               Network Address Translation= SUA Only
               Address Mapping Set= N/A

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

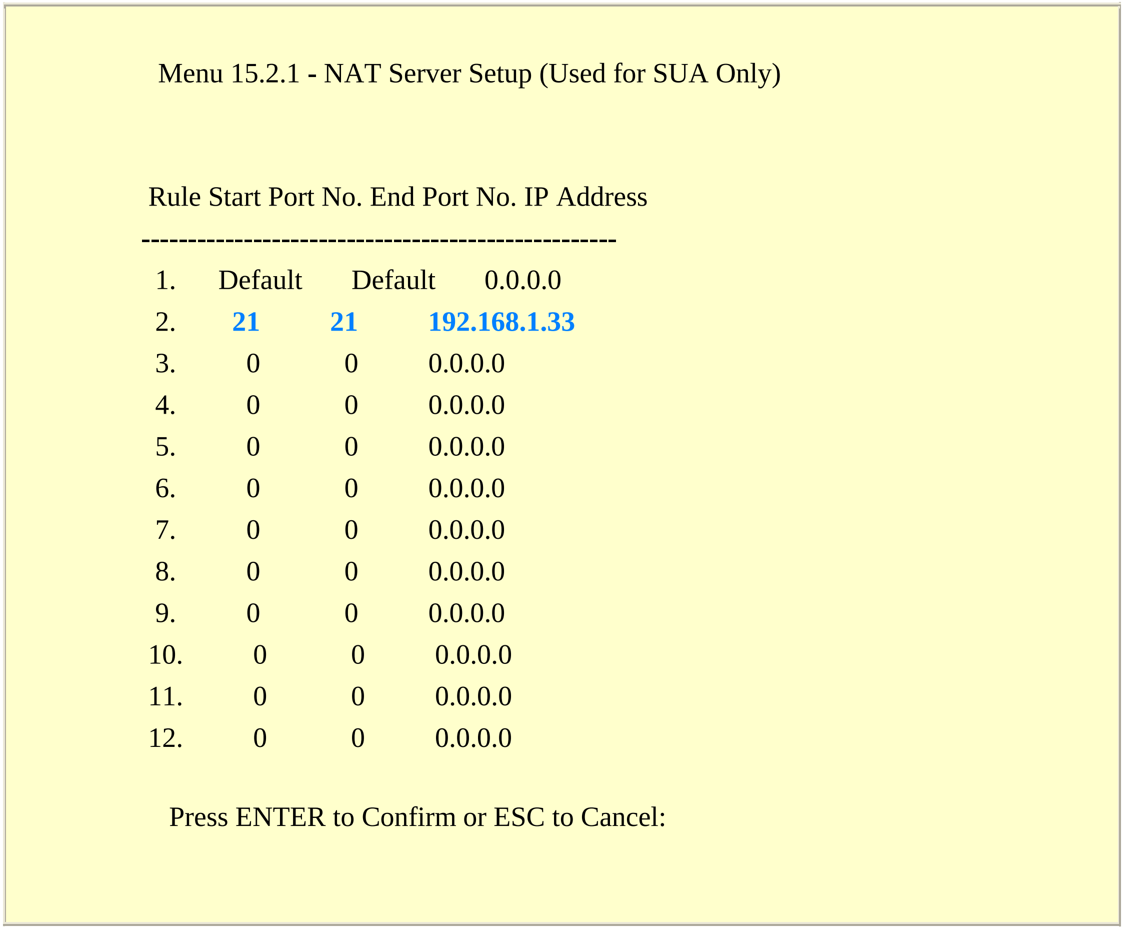
From Menu 4 shown above simply choose the **SUA Only** option from the **NAT** field. This is the **Many-to-One** mapping discussed earlier. The SUA read only option from the NAT field in menu 4 and 11.3 is specifically pre-configured to handle this case.

2. Internet Access with an Internal Server



Internet Access using NAT Many-to-One plus a Server Set

In this case, we do exactly as above (use the convenient pre-configured SUA Only set) and also go to Menu 15.2.1-**NAT Server Setup (Used for SUA Only)** to specify the Internet Server behind the NAT as shown in the NAT as shown below.

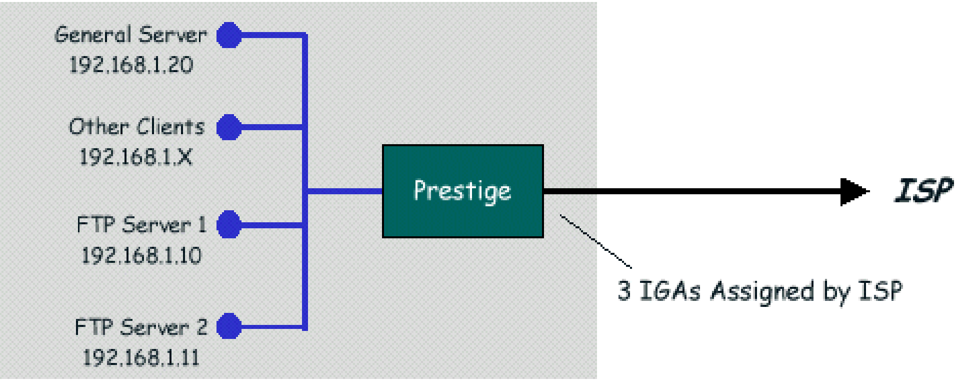


```
   Menu 15.2.1 - NAT Server Setup (Used for SUA Only)


  Rule Start Port No. End Port No. IP Address
 --------------------------------------------------
   1.    Default    Default    0.0.0.0
   2.      21         21     192.168.1.33
   3.      0          0      0.0.0.0
   4.      0          0      0.0.0.0
   5.      0          0      0.0.0.0
   6.      0          0      0.0.0.0
   7.      0          0      0.0.0.0
   8.      0          0      0.0.0.0
   9.      0          0      0.0.0.0
  10.      0          0      0.0.0.0
  11.      0          0      0.0.0.0
  12.      0          0      0.0.0.0

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

3. Using Multiple Global IP addresses for clients and servers (One-to-One, Many-to-One, Server Set mapping types are used)



Mapping Multiple IGAs for clients and servers

In this case we have 3 IGAs (IGA1, IGA2 and IGA3) from the ISP. We have two very busy internal FTP servers and also an internal general server for the web and mail. In this case, we want to assign the 3 IGAs by the following way using 4 NAT rules.

- Rule 1 (One-to-One type) to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1.
- Rule 2 (One-to-One type) to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2.
- Rule 3 (Many-to-One type) to map the other clients to IGA3.
- Rule 4 (Server type) to map a web server and mail server with ILA3 (192.168.1.20) to IGA3. Type **Server** allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

Step 1:

In this case, we need to configure Address Mapping Set 1 from **Menu 15.1-Address Mapping Sets**. Therefore we must choose the **Full Feature** option from the **NAT** field in menu 4 or menu 11.3, and assign IGA3 to P-660 WAN IP Address.

```
                Menu 4 - Internet Access Setup

              ISP's Name= CHT
              Encapsulation= PPPoE
              Multiplexing= LLC-based
              VPI #= 0
              VCI #= 33
              ATM QoS Type= CBR
                 Peak Cell Rate (PCR)= 0
                 Sustain Cell Rate (SCR)= 0
                 Maximum Burst Size (MBS)= 0
              My Login= N/A
              My Password= N/A
              ENET ENCAP Gateway= N/A
              IP Address Assignment= Static
              IP Address= IGA3
              Network Address Translation= Full Feature
              Address Mapping Set= 1

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

Step 2:

Go to menu 15.1 and choose 1 (not 255, SUA this time) to begin configuring this new set. Enter a **Set Name**, choose the **Edit Action** and then select 1 from **Select Rule** field. Press [ENTER] to confirm. See the following setup for the four rules in our case.

Rule 1 Setup: Select **One-to-One** type to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1.

```
  Menu 15.1.1.1 -   - Rule 1
Type: One-to-One
Local IP:
Start= 192.168.1.10
End   = N/A
Global IP:
  Start= [Enter IGA1]
  End   = N/A

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

Rule 2 Setup: Selecting **One-to-One** type to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2.

```
Menu 15.1.1.2 -   - Rule 2

Type: One-to-One

Local IP:
  Start= 192.168.1.11
  End   = N/A

Global IP:
  Start= [Enter IGA2]
  End   = N/A

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

Rule 3 Setup: Select **Many-to-One** type to map the other clients to IGA3.

```
Menu 15.1.1.3 -   - Rule 3

Type: Many-to-One

Local IP:
  Start= 0.0.0.0
  End   = 255.255.255.255

Global IP:
  Start= [Enter IGA3]
  End   = N/A


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

Rule 4 Setup: Select **Server type** to map our web server and mail server with ILA3 (192.168.1.20) to IGA3.

```
               Menu 15.1.1.4 -   - Rule 4

             Type: Server

             Local IP:
               Start= N/A
               End   = N/A

             Global IP:
               Start=[Enter IGA3]
               End   = N/A


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

When we have configured all four rules Menu 15.1.1 should look as follows.

```
             Menu 15.1.1 - Address Mapping Rules

  Set Name= Example3

Idx   Local Start IP    Local End IP      Global Start IP   Global End IP     Type
---   ---------------   ---------------   ---------------   ---------------   ------
  1.   192.168.1.10                        [IGA1]                              1-1
  2.   192.168.1.11                        [IGA2]                              1-1
  3.   0.0.0.0          255.255.255.255   [IGA3]                              M-1
  4.                                       [IGA3]                              Server
  5.
  6.
  7.
  8.
  9.
10.


                 Press ESC or RETURN to Exit:
```

Step 3:

Now we configure all other incoming traffic to go to our web server aand mail server from **Menu 15.2.2 - NAT Server Setup** (not Set 1, Set 1 is used for SUA Only case).

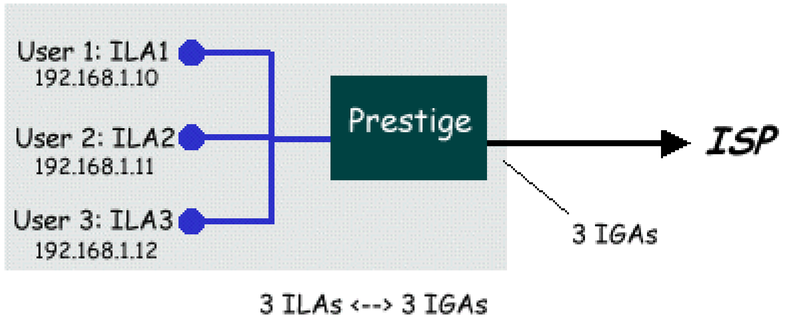
```
                 Menu 15.2.2 - NAT Server Setup


          Rule Start Port No. End Port No. IP Address
         --------------------------------------------------
           1.     Default       Default       0.0.0.0
           2.       80            80        192.168.1.20
           3.       25            25        192.168.1.20
           4.        0             0        0.0.0.0
           5.        0             0        0.0.0.0
           6.        0             0        0.0.0.0
           7.        0             0        0.0.0.0
           8.        0             0        0.0.0.0
           9.        0             0        0.0.0.0
          10.        0             0        0.0.0.0
          11.        0             0        0.0.0.0
          12.        0             0        0.0.0.0

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

4. Support Non NAT Friendly Applications

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user login to the server using a unique global IP address. The following figure illustrates this.



3 ILAs map to 3 IGAs using Many-to-Many No Overload or One-to-One type

One rule configured for using **Many-to-Many No Overload** mapping type is shown below.

Menu 15.1.1.1 - - Rule 1
Type: **Many-to-Many No Overload**
Local IP:
Start= **192.168.1.10**
End = **192.168.1.12**
Global IP:
Start= **[Enter IGA1]**
End = **[Enter IGA3]**
Press ENTER to Confirm or ESC to Cancel:

The three rules configured for using **One-to-One** mapping type is shown below.

Menu 15.1.1.1 - - Rule 1
Type: **One-to-One**
Local IP:
Start= **192.168.1.10**
End = N/A
Global IP:
Start= **[Enter IGA1]**
End = N/A
Press ENTER to Confirm or ESC to Cancel:

Menu 15.1.1.2 - - Rule 2

```
            Type: One-to-One
             Local IP:
                 Start= 192.168.1.11
                 End   = N/A
             Global IP:
                 Start= [Enter IGA2]
                 End   = N/A
        Press ENTER to Confirm or ESC to Cancel:
```

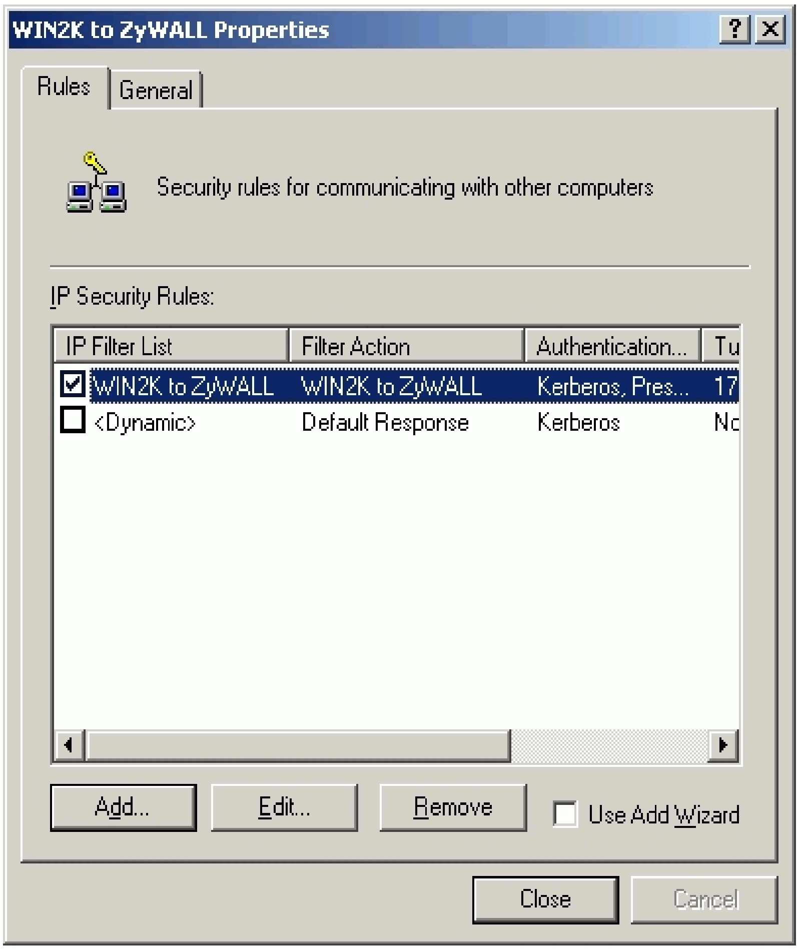
```
              Menu 15.1.1.3 -   - Rule 3
          Type: One-to-One
           Local IP:
                 Start= 192.168.1.12
                 End   = N/A
            Global IP:
                 Start= [Enter IGA3]
                 End   = N/A
             Press ENTER to Confirm or ESC to Cancel:
```

6. About Filter & Filter Examples

How does ZyXEL filter work?

Filter Structure

The P-660 allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port. The following diagram illustrates the logic flow when executing a filter rule.



Security rules for communicating with other computers

IP Security Rules:

	IP Filter List	Filter Action	Authentication...	Tu
☑	WIN2K to ZyWALL	WIN2K to ZyWALL	Kerberos, Pres...	17
□	<Dynamic>	Default Response	Kerberos	Nc

□ Use Add Wizard

Filter Types and SUA

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 the protocol category; they act on the IP and IPX packets.

In order to allow 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 the P-660 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:

- LAN device and protocol input filter sets.
- WAN protocol call and output filter sets.
- If SUA is enabled, SUA converts the source IP address from 192.168.1.33 to 203.205.115.6 and port number from 1023 to 4034.

- WAN device output and call filter sets.

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

WAN device input filter sets.

If SUA is enabled, SUA converts the destination IP address from 203.205.115.6 to 92.168.1.33 and port number from 4034 to 1023.

WAN protocol input filter sets.

LAN device and protocol output filter sets.

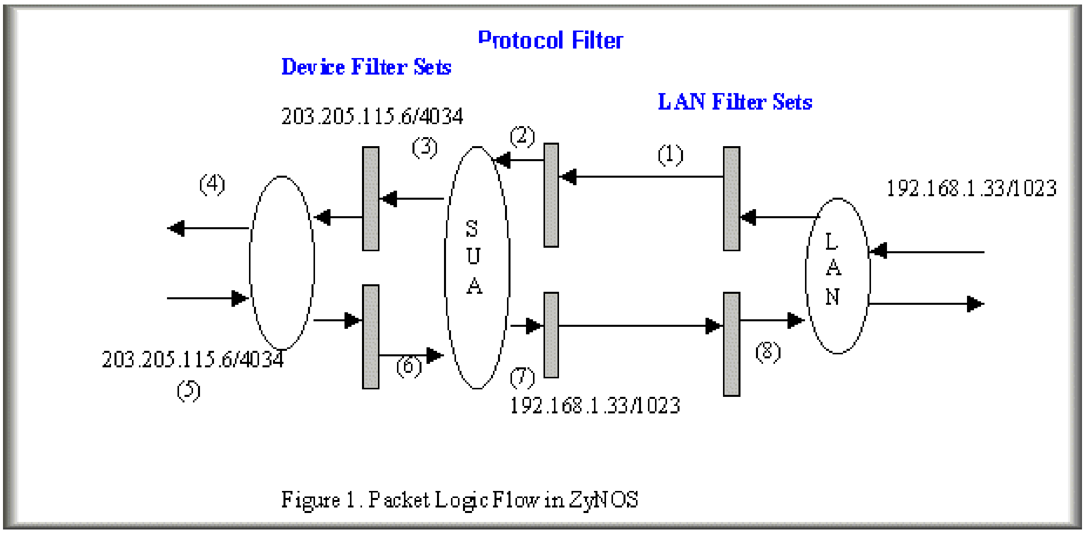


Figure 1. Packet Logic Flow in ZyNOS

Generic and **TCP/IP (and IPX)** filter rules are 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 new fields are shown below.

Menu 3.1:

```
              Menu 3.1 - General Ethernet Setup

           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= LAN       Route= IP
          Active= Yes              Bridge= No

        Encapsulation= PPP       Edit PPP Options= No
        Incoming:                Rem IP Addr= ?
        Rem Login= test          Edit IP/IPX/Bridge= No
        Rem Password= ********
        Outgoing:                Session Options:
       My Login= testt           Edit Filter Sets= Yes
       My Password= *****
        Authen= CHAP/PAP
      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=
```

SMT will also prevent you from entering a protocol filter set configured in Menu 21 to the **device filters** field in Menu 3.1, 11.5, 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 use.

In order to avoid operational problems later, the P-660 will disable its routing/bridging functions if there is an inconsistency among its filter rules.

Filter Examples

1. A filter for blocking the web service
2. A filter for blocking a specific client
3. A filter for blocking a specific MAC address
4. A filter for blocking the NetBIOS packets

A filter for blocking the web service

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.

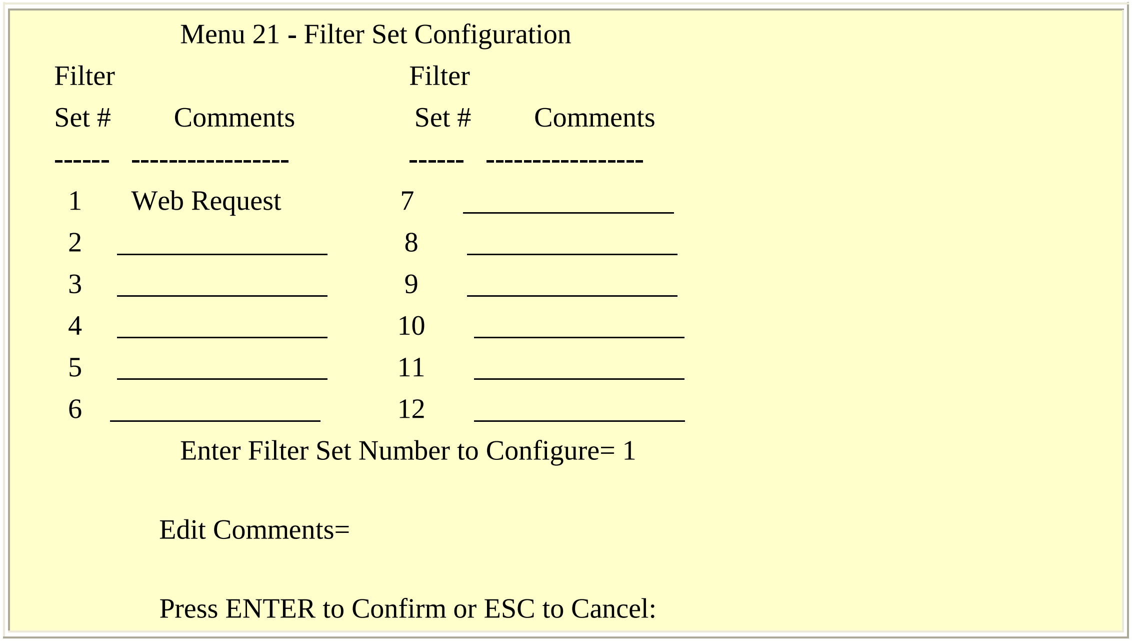
1. Create a filter set in Menu 21, e.g., set 1

2. 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

3. Apply the filter set in menu 4

1. Create a filter set in Menu 21

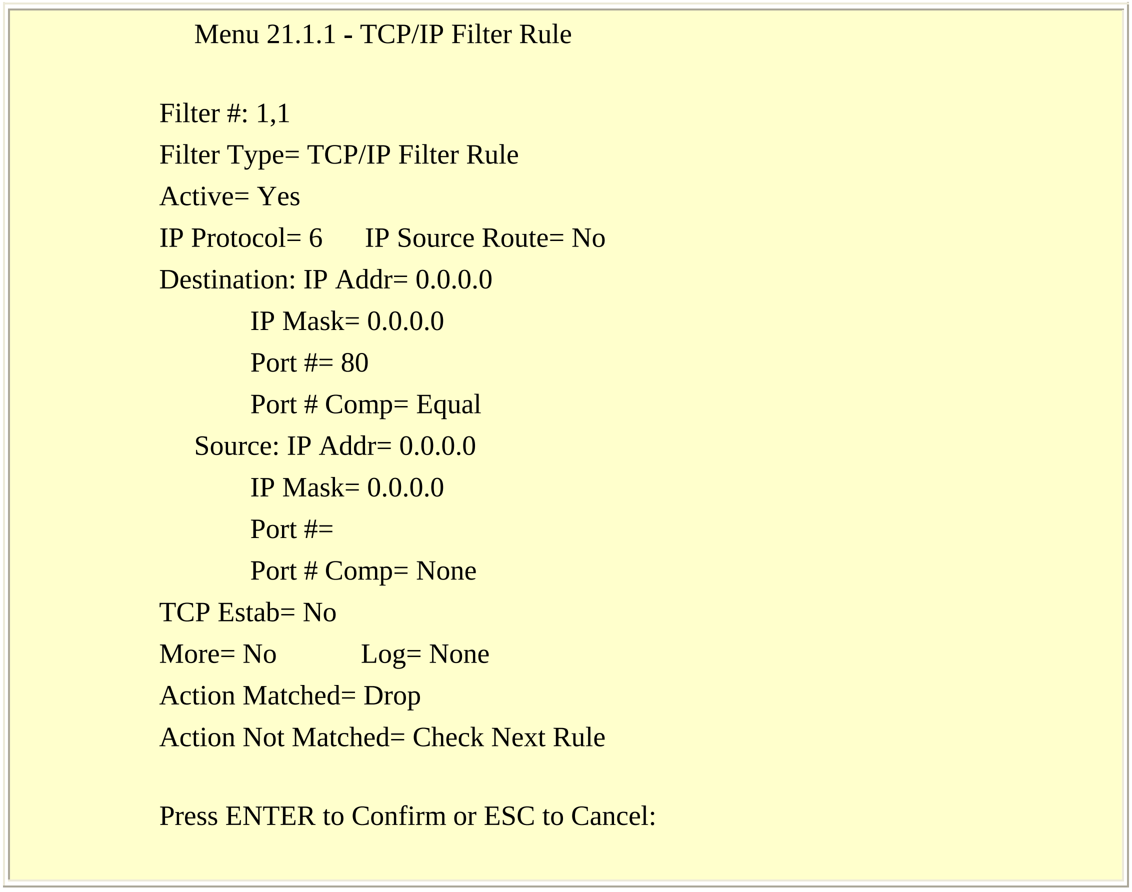


```
                 Menu 21 - Filter Set Configuration
  Filter                              Filter
  Set #       Comments                 Set #       Comments
  ------   -----------------          ------   -----------------
    1      Web Request               7      ________________
    2    ________________            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:
```

2. Rule 1 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 #=
                            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:
```

3.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 #=
                           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:
```

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

```
                 Menu 21.1.2 - 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 #=
                           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:
```

5. 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
```

6. Apply the filter set to the **'Output Protocol Filter Set'** in the remote node setup

A filter for blocking a specific client

Configuration

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

```
                   Menu 21 - Filter Set Configuration

     Filter                          Filter
     Set #       Comments               Set #       Comments
     ------   -----------------         ------   -----------------
       1       Block a client             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:
```

2. One rule 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 #=
                    Port # Comp= None
          Source: IP Addr= 192.168.1.5
                    IP Mask= 255.255.255.255
                    Port #=
                    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:
```

Key Settings:

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

3. Apply the filter set number '1' to the **'Output Protocol Filter Set'** field in the remote node setup.

A filter for blocking a specific MAC address

This configuration example shows you how to use a Generic Filter to block a specific MAC address of the LAN.

Before you Begin

Before you configure the filter, you need to know the MAC address of the client first. The MAC address can be provided by the NICs. If there is the LAN packet passing through the P-660 you can identify the uninteresting MAC address from the P-660's LAN packet trace. Please have a look at the following example to know the trace of the LAN packets.

```
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on

Now a client on the LAN is trying to ping Prestige………

ras> sys trcp sw off
ras> sys trcp disp

TIME:   37c060   enet0-RECV len:74 call=0
   0000: [00 a0 c5 01 23 45] [00 80 c8 4c ea 63] 08 00 45 00
   0010: 00 3c eb 0c 00 00 20 01 e3 ea ca 84 9b 5d ca 84
   0020: 9b 63 08 00 45 5c 03 00 05 00 61 62 63 64 65 66
   0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
   0040: 77 61 62 63 64 65 66 67 68 69

TIME:   37c060   enet0-XMIT len:74 call=0
   0000: [00 80 c8 4c ea 63] [00 a0 c5 01 23 45] 08 00 45 00
   0010: 00 3c 00 07 00 00 fe 01 f0 ef ca 84 9b 63 ca 84
   0020: 9b 5d 00 00 4d 5c 03 00 05 00 61 62 63 64 65 66
   0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
   0040: 77 61 62 63 64 65 66 67 68 69
```

The detailed format of the Ethernet Version II:

```
+ Ethernet Version II
    - Address: 00-80-C8-4C-EA-63 (Source MAC) ----> 00-A0-C5-23-45
      (Destination MAC)
    - Ethernet II Protocol Type: IP
+ Internet Protocol
    - Version (MSB 4 bits): 4
    - Header length (LSB 4 bits): 5
    - Service type: Precd=Routine, Delay=Normal, Thrput=Normal, Reli=Normal
    - Total length: 60 (Octets)
    - Fragment ID: 60172
    - Flags: May be fragmented, Last fragment, Offset=0 (0x00)
    - Time to live: 32 seconds/hops
    - IP protocol type: ICMP (0x01)
    - Checksum: 0xE3EA
    - IP address 202.132.155.93   (Source IP address) ---->
      202.132.155.99(Destination IP address)
    - No option
+ Internet Control Message Protocol
    - Type: 8 - Echo Request
    - Code: 0
    - Checksum: 0x455C
    - Identifier: 768
    - Sequence Number: 1280
    - Optional Data: (32 bytes)
```

Configurations

From the above first trace, we know a client is trying to ping request the P-660 router. And from the second trace, we know the P-660 router will send a reply to the client accordingly.   The following sample filter will utilize the 'Generic Filter Rule' to block the MAC address **[00 80 c8 4c ea 63]**.

1. First, from the incoming LAN packet we know the uninteresting source MAC address starts at the 7th Octet

```
TIME:   37c060   enet0-RECV len:74 call=0
  0000: [00 a0 c5 01 23 45] [00 80 c8 4c ea 63] 08 00 45 00
  0010: 00 3c eb 0c 00 00 20 01 e3 ea ca 84 9b 5d ca 84
  0020: 9b 63 08 00 45 5c 03 00 05 00 61 62 63 64 65 66
  0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
  0040: 77 61 62 63 64 65 66 67 68 69
```

2. We are now ready to configure the 'Generic Filter Rule' as below.

```
              Menu 21.1.1 - Generic Filter Rule

               Filter #: 1,1
               Filter Type= Generic Filter Rule
               Active= Yes
               Offset= 6
               Length= 6
               Mask= ffffffffffff
               Value= 0080c84cea63
```

```
        More= No          Log= None
        Action Matched= Drop
        Action Not Matched= Forward
```

Key Settings:

- Generic Filter Ruls
  Set the 'Filter Type' to 'Generic Filter Rule'

- Active
  Turn 'Active' to 'Yes'

- Offset (in bytes)
  Set to '6' since the source MAC address starts at 7th octets we need to skip the first octets of the destination MAC address.

Length (in bytes)
Set to '6' since MAC address has 6 octets.

Mask (in hexadecimal)
Specify the value that the P-660 will logically qualify (logical AND) the data in the packet.
Since the Length is set to 6 octets the Mask for it should be 12 hexadecimal numbers. In this case, we intent to set to 'ffffffffffff' to mask the incoming source MAC address, [00 80 c8 4c ea 63].

- Value (in hexadecimal)
  Specify the MAC address **[00 80 c8 4c ea 63]** that the P-660 should use to compare with the masked packet. If the result from the masked packet matches the 'Value', then the packet is considered matched.

- Action Matched=
  Enter the action you want if the masked packet matches the 'Value'. In this case, we will drop it.

- Action Not Matched=
  Enter the action you want if the masked packet does not match the 'Value'. In this case, we will forward it. If you want to configure more rules please select 'Check Next Rule' to start configuring the next new rule. However, please note that the 'Filter Type' must be also 'Generic Filter Rule' but not others. Because the Generic and TCPIP (IPX) filter rules must be in different filter sets.

```
          Menu 21.1.2 - Generic Filter Rule

          Filter #: 1,2
          Filter Type= Generic Filter Rule
          Active= Yes
          Offset= 6
          Length= 6
          Mask= ffffffffffff
          Value= 0080c810234a
          More= No          Log= None
          Action Matched= Drop
          Action Not Matched= Forward
```

You can now apply it to the **'General Ethernet Setup'** in Menu 3.1. Please note that the **'Generic Filter'** can only be applied to the **'Device Filter'** but not the **'Protocol Filter'** that is used for configuring the TCPIP and IPX filters.

```
          Menu 3.1 - General Ethernet Setup

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

A filter for blocking the NetBIOS packets

Introduction

The NETBIOS protocol is used to share a Microsoft comupter of a workgroup. For the security concern, the NetBIOS connection to a outside host is blocked by P-660 router as factory defaults. Users can remove the filter sets applied to menu 3.1 and menu 4.1 for activating the NetBIOS services. The details of the filter settings are described as follows.

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_WAN                7       _______________
     2      NetBIOS_LAN                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_WAN' 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
```

- 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.

```
             Menu 21.2 - 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=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
```

Apply the first filter set 'NetBIOS_WAN' to the **'Output Protocol Filter'** in the remote node setup.

Configure the second filter set 'NetBIOS_LAN' 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:
```

1. 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:
```

2. 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
```

3. Apply the filter set 'NetBIOS_LAN' in the **'Input protocol filters='** in the Menu 3 for blocking the packets from LAN

```
          Menu 3.1 - General Ethernet Setup

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

7. Using the Dynamic DNS (DDNS)

- What is DDNS?

The DDNS service, an IP Registry provides a public central database where information such as email addresses, hostnames, IPs etc. can be stored and retrieved. This solves the problems if your DNS server uses an IP associated with dynamic IPs.

Without DDNS, we always tell the users to use the WAN IP of the P-660 to access the internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-660.

When the ISP assigns the P-660 a new IP, the P-660 must inform the DDNS server the change of this IP so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

The DDNS server stores password-protected email addresses with IPs and hostnames and accepts queries based on email addresses. So, there must be an email entry in the P-660 menu 1.

The DDNS servers the P-660 supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

- Setup the DDNS

1. Before configuring the DDNS settings in the P-660, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you have a hostname for your internal server and a password using to update the IP to the DDNS server.
2. Toggle '**Configure Dynamic DNS**' option to '**Yes**' and press ENTER for configuring the settings of the DDNS in menu 1.1.

```
Menu 1 - General Setup

  System Name= P-660
  Location=
  Contact Person's Name=
  Domain Name=
  Edit Dynamic DNS= Yes

  Route IP= Yes
  Bridge= No
  Menu 1.1 - Configure Dynamic DNS

 Service Provider= WWW.DynDNS.ORG
 Active= Yes
 Host= [the local server's host name]
 EMAIL= [your email address]
 User=
 Password= ********
 Enable Wildcard= No
```

Key Settings for using DDNS function:

Option	Description
Service Provider	Enter the DDNS server in this field. Currently, we support WWW.DYNDNS.ORG.
Active	Toggle to **'Yes'**.
Host	Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw.
EMAIL	Enter the email address you give to the DDNS server.
User	Enter the user name that
Password	Enter the password that the DDNS server gives to you.
Enable Wildcard	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is http://www.dyndns.org/.

8. Network Management Using SNMP

- SNMP Overview

The Simple Network Management Protocol (SNMP) is an applications-layer protocol used to exchange the management information between network devices (e.g., routers). By using SNMP, network administrators can more easily manage network performance, find and solve network problems. The SNMP is a member of the TCP/IP protocol suite, it uses the UDP to exchange messages between a management Client and an Agent, residing in a network node.

There are two versions of SNMP: Version 1 and Version 2. ZyXEL supports SNMPv1. Most of the changes introduced in Version 2 increase SNMP's security capabilities. SNMP encompasses three main areas:

1. A small set of management operations.
2. Definitions of management variables.
3. Data representation.

The operations allowed are: **Get**, **GetNext**, **Set**, and **Trap**. These functions operates on variables that exist in network nodes. Examples of variables include statistic counters, node port status, and so on. All of the SNMP management functions are carried out through these simple operations. No action operations are available, but these can be simulated by the setting of flag variables. For example, to reset a node, a counter variable named 'time to reset' could be set to a value, causing the node to reset after the time had elapsed.

SNMP variables are defined using the OSI Abstract Syntax Notation One (ASN.1). ASN.1 specifies how a variable is encoded in a transmitted data frame; it is very powerful because the encoded data is self-defining. For example, the encoding of a text string includes an indication that the data unit is a string, along with its length and value. ASN.1 is a flexible way of defining protocols, especially for network management protocols where nodes may support different sets of manageable variables.

The net of variables that each node supports is called the ***Management Information Base*** (MIB). The MIB is made up of several parts, including the Standard MIB, specified as part of SNMP, and Enterprise Specific MIB, which are defined by different manufacturer for hardware specific management.

The current Internet-standard MIB, MIB-II, is defined in RFC 1213 and contains 171 objects. These objects are grouped by protocol (including TCP, IP, UDP, SNMP, and other categories, including 'system' and 'interface.'

The Internet Management Model is as shown in figure 1. Interactions between the NMS and managed devices can be any of four different types of commands:

Reads

> Read is used to monitor the managed devices, NMSs read variables that are maintained by the devices.

Writes

> Write is used to control the managed devices, NMSs write variables that are stored in the managed devices.

Traversal operations

NMSs use these operations to determine which variables a managed device supports and to sequentially gather information from variable tables (such as IP routing table) in managed devices.

Traps

The managed devices to asynchronously report certain events to NMSs use trap.

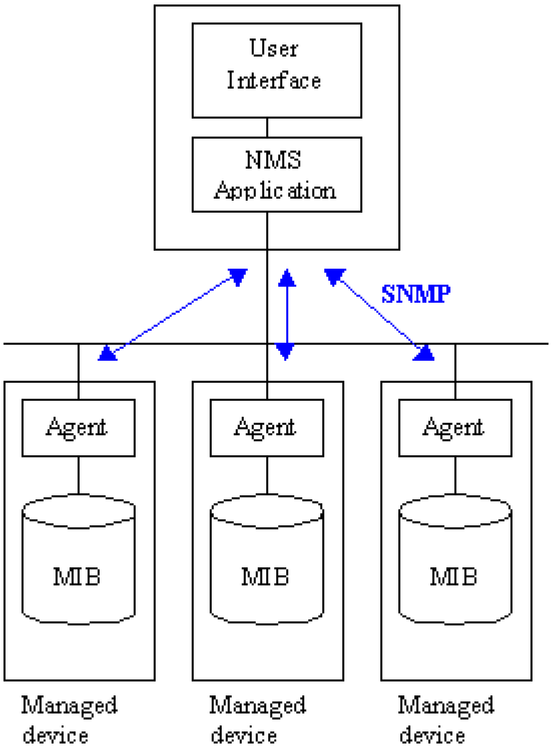


Figure 1: SNMP Management Model

- SNMPv1 Operations

SNMP itself is a simple request/response protocol. 4 SNMPv1 operations are defined as below.

- **Get**
  Allows the NMS to retrieve an object variable from the agent.
- **GetNext**
  Allows the NMS to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a NMS wants to retrieve all elements of a table

from an agent, it initiates a Get operation, followed by a of GetNext operations.

- **Set**
  Allows the NMS to set values for object variables within an agent.
- **Trap**
  Used by the agent to inform the NMS of some events.

The SNMPv1 messages contains two part. The first part contains a version and a community name. The second part contains the actual SNMP protocol data unit (PDU) specifying the operation to be performed (Get, Set, and so on) and the object values involved in the operation. The following figure shows the SNMPv1 message format.

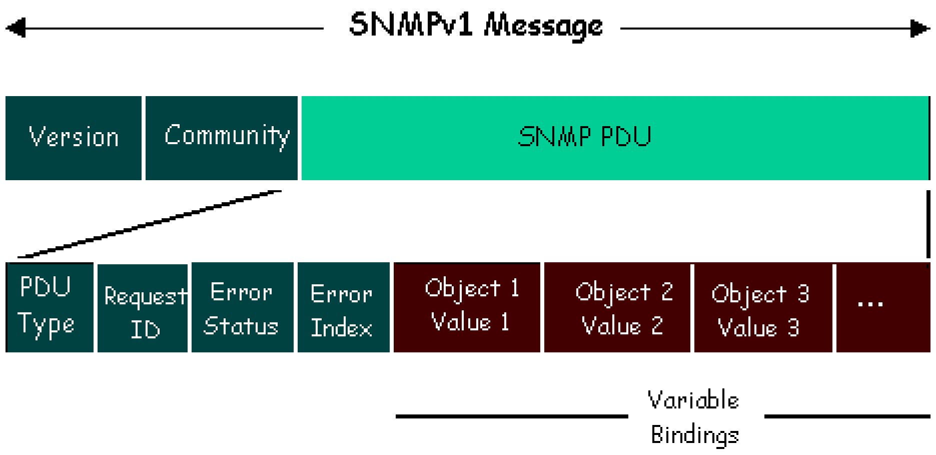


Figure 2: SNMPv1 Message Format

The SNMP PDU contains the following fields:

- **PDU type** Specifies the type of PDU.
- **Request ID** Associates requests with responses.
- **Error status** Indicates an error and an error type.
- **Error index** Associates the error with a particular object variable.
- **Variable-bindings** Associates particular object with their value.

- ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some P-660 routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. Further, users can also add ZyXEL's private MIB in the NMS to monitor and control additional system variables. The ZyXEL's private MIB tree is shown in figure 3. For

SNMPv1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

Some traps are sent to the SNMP manager when anyone of the following events happens:

1. coldStart (defined in RFC-1215) :

   If the machine coldstarts, the trap will be sent after booting.

1. warmStart (defined in RFC-1215) :

   If the machine warmstarts, the trap will be sent after booting.

2. linkDown (defined in RFC-1215) :

   If any link of IDSL or WAN is down, the trap will be sent with the port number . The port number is its interface index under the interface group.

3. linkUp (defined in RFC-1215) :

   If any link of IDSL or WAN is up, the trap will be sent with the port number . The port number is its interface index under the interface group.

4. authenticationFailure (defined in RFC-1215) :

   When receiving any SNMP get or set requirement with wrong community, this trap is sent to the manager.

5. whyReboot (defined in ZYXEL-MIB) :

When the system is going to restart (warmstart), the trap will be sent with the reason of restart before rebooting.

(i) For intentional reboot :

In some cases (download new files, CI command "sys reboot", ...), reboot is done intentionally. And traps with the message "System reboot by user !" will be sent.

(ii) For fatal error :

System has to reboot for some fatal errors. And traps with the message of the fatal code will be sent.

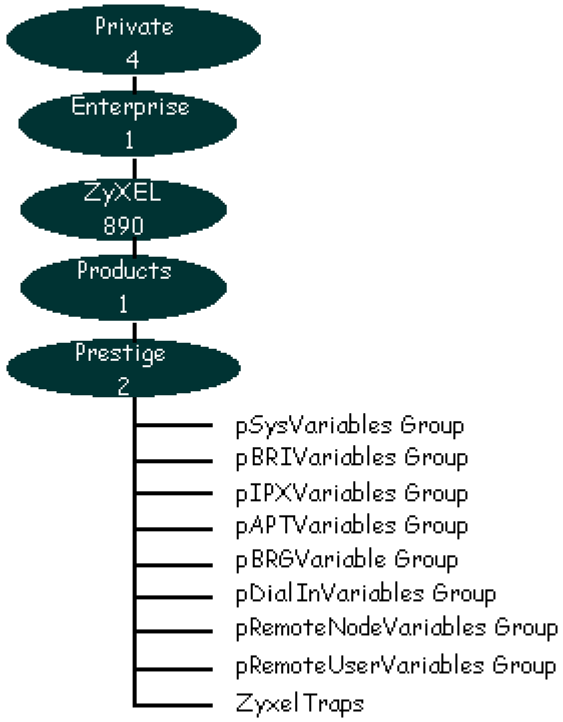
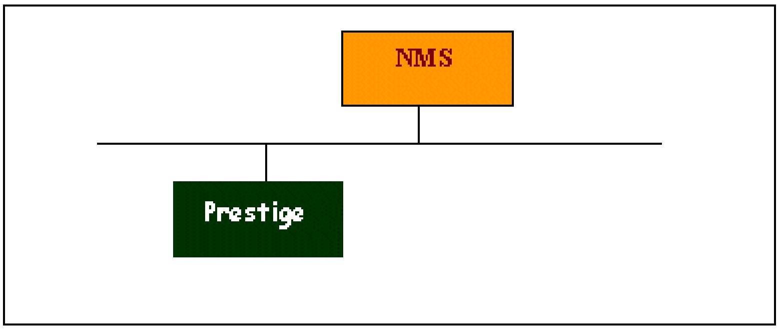


Figure 3: ZyXEL Private MIB Tree

- ***Downloading ZyXEL's private MIB***

- Configure the P-660 for SNMP



The SNMP related settings in P-660 are configured in menu 22, SNMP Configuration. The following steps describe a simple setup procedure for configuring all SNMP settings.

```
                 Menu 22 - SNMP Configuration

          SNMP:
```

```
          Get Community= public
          Set Community= public
          Trusted Host= 192.168.1.33
          Trap:
            Community= public
            Destination= 192.168.1.33


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

Key Settings:

Option	Descriptions
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
Trusted Host	Enter the IP address of the NMS. The P-660 will only respond to SNMP messages coming from this IP address. **If 0.0.0.0 is entered, the P-660 will respond to all NMS managers.**
Trap Community	Enter the community name in each sent trap to the NMS. This Trap Community must match what the NMS is expecting. The default is 'public'.
Trap Destination	Enter the IP address of the NMS that you wish to send the traps to. **If 0.0.0.0 is entered, the P-660 will not send trap any NMS manager.**

9. Using syslog

- P-660 Setup
- UNIX Setup
- ZyXEL Syslog Message Format

P-660 Setup

```
   Menu 24.3.2 - System Maintenance - UNIX Syslog and Accounting

          UNIX Syslog:
          Active= Yes
          Syslog IP Address= 192.168.1.33
```

```
        Log Facility= Local 1

        Types:
        CDR= No
        Packet triggered= No
        Filter log= No
        PPP log= No
```

Configuration:

1. **Active**, use the space bar to turn on the syslog option.
2. **Syslog IP Address**, enter the IP address of the UNIX server that you wish to send the syslog.
3. **Log Facility,** use the space bar to toggle between the 7 different local options.
4. **Types**, use the space bar to toggle the logs we are going to record.

UNIX Setup

1. Make sure that your syslog starts with ***-r*** argument.

-r, this option will enable the facility to receive message from the network using an Internet domain socket with the syslog services. The default setting is not enabled.

2. Edit the file **/etc/syslog.conf** by adding the following line at the end of the **/etc/syslog.conf** file.

```
local1.*    /var/log/zyxel.log
```

Where /var/log/zyxel.log is the full path of the log file.

3. Restart syslogd.

ZyXEL Syslog Message Format

CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter log	No filters are logged when this field is set to **No**. Filters with the individual filter Log field set to Yes are logged when this field is set to **Yes**.
PPP log	PPP events are logged when this field is set to **Yes**.

1. CDR log(call messages)

Format:

sdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
  C01 Incoming Call xxxxBps xxxxx (L2TP,xxxxx means Remote Call ID)
  C01 Incoming Call xxxx (means connected speed) xxxxx (means Remote Call ID)
  L02 Tunnel Connected(L2TP)
  C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call ID)
  C02 CLID call refused
  L02 Call Terminated
  C02 Call Terminated

Example:

```
Feb 14 16:57:17 192.168.1.1 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 18,
C01 Incoming Call OK
Feb 14 17:07:18 192.168.1.1 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 18,
C02 Call Terminated
```

2. Packet triggered log

Format:

sdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server

Example:

```
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696
a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd
40000020405b4
```

3. Filter log

This message is available when the **'Log'** is enabled in the filter rule setting. The message consists of the packet header and the log of the filter rules.

Format:

sdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx]S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).

Src: Source Address
Dst: Destination Address
prot: Protocol (TCP,UDP,ICMP)
spo: Source port
dpo: Destination port

Example:

```
Jul 19 14:44:09 192.168.1.1 ZyXEL Communications Corp.: IP[Src=202.132.154.1
Dst=192.168.1.33 UDP spo=0035   dpo=05d4]}S03>R01mF
Jul 19 14:44:13 192.168.1.1 ZyXEL Communications Corp.: IP[Src=192.168.1.33
Dst=202.132.154.1 ICMP]}S03>R01mF
```

4. PPP Log

Format:

sdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /IPXCP

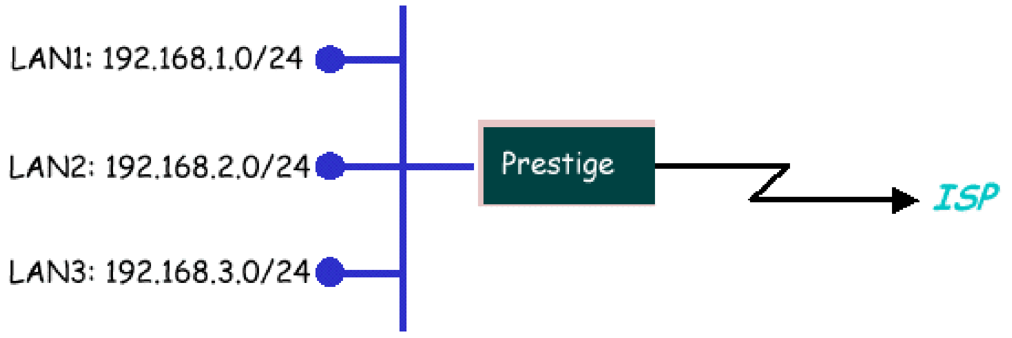
Example:

```
Jul 19 11:43:25 192.168.1.1 ZyXEL Communications Corp.: ppp:LCP Starting
Jul 19 11:43:29 192.168.1.1 ZyXEL Communications Corp.: ppp:IPCP Starting
Jul 19 11:43:34 192.168.1.1 ZyXEL Communications Corp.: ppp:CCP Starting
Jul 19 11:43:38 192.168.1.1 ZyXEL Communications Corp.: ppp:BACP Starting
Jul 19 11:43:43 192.168.1.1 ZyXEL Communications Corp.: ppp:IPCP Opening
Jul 19 11:43:51 192.168.1.1 ZyXEL Communications Corp.: ppp:CCP Opening
Jul 19 11:43:55 192.168.1.1 ZyXEL Communications Corp.: ppp:BACP Opening
Jul 19 11:44:00 192.168.1.1 ZyXEL Communications Corp.: ppp:LCP Closing
Jul 19 11:44:05 192.168.1.1 ZyXEL Communications Corp.: ppp:IPCP Closing
Jul 19 11:44:09 192.168.1.1 ZyXEL Communications Corp.: ppp:CCP Closing
Jul 19 11:44:14 192.168.1.1 ZyXEL Communications Corp.: ppp:BACP Closing
```

10. Using IP Alias

- What is IP Alias ?

In a typical environment, a LAN router is required to connect two local networks. The P-660 can connect three local networks to the ISP or a remote node, we call this function as **'IP Alias'**. In this case, an internal router is not required. For example, the network manager can divide the local network into three networks and connect them to the Internet using P-660's single user account. See the figure below.



The Prestige's IP Alias connects three local networks to the Internet

The P-660 supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured in menu 3.2 as usual. The second and third networks that we call **'IP Alias 1'** and **'IP Alias 2'** can be configured in menu 3.2.1-IP Alias Setup.

There are three internal virtual LAN interfaces for the P-660 to route the packets from/to the three networks correctly. They are **enif0** for the major network, **enif0:0** for the IP alias 1 and **enif0:1** for the IP alias 2. Therefore, three routes are created in the P-660 as shown below when the three networks are configured. If the P-660's DHCP is also enabled, the IP pool for the clients can be any of the three networks.

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
```

```
ras> ip ro st
Dest            FF Len Interface   Gateway          Metric stat Timer   Use
192.168.3.0      00 24   enif0:1     192.168.3.1       1     041b 0      0
192.168.2.0      00 24   enif0:0     192.168.2.1       1     041b 0      0
192.168.1.0      00 24   enif0      192.168.1.1       1     041b 0      0
ras>
```

Two new protocol filter interfaces in menu 3.2.1 allow you to accept or deny LAN packets from/to the IP alias 1 and IP alias 2 go through the P-660. The filter set in menu 3.1 is used for main network configured in menu 3.2.

- IP Alias Setup

1. Edit the first network in menu 3.2 by configuring the P-660's first LAN IP address.

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

     DHCP Setup
          DHCP= Server
          Client IP Pool Starting Address= 192.168.1.33
          Size of Client IP Pool= 6
          Primary DNS Server= 168.95.1.1
          Secondary DNS Server= 168.95.192.1
          Remote DHCP Server= N/A
      TCP/IP Setup:
          IP Address= 192.168.1.1
          IP Subnet Mask= 255.255.255.0
          RIP Direction= Both
             Version= RIP-1
          Multicast= None
          IP Policies=
          Edit IP Alias= Yes

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

Key Settings:

DHCP Setup	If the P-660's DHCP server is enabled, the IP pool for the clients can be any of the three networks.
TCP/IP Setup	Enter the first LAN IP address for the P-660. This will create the first route in the enif0 interface.

Edit IP Alias	Toggle to **'Yes'** to enter menu 3.2.1 for setting up the second and third networks.

2. Edit the second and third networks in menu 3.2.1 by configuring the P-660's second and third LAN IP addresses.

```
             Menu 3.2.1 - IP Alias Setup

         IP Alias 1= Yes
         IP Address= 192.168.2.1
         IP Subnet Mask= 255.255.255.0
         RIP Direction= None
         Version= RIP-1
         Incoming protocol filters=
         Outgoing protocol filters=
        IP Alias 2= Yes
         IP Address= 192.168.3.1
         IP Subnet Mask= 255.255.255.0
         RIP Direction= None
         Version= RIP-1
         Incoming protocol filters=
         Outgoing protocol filters=

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

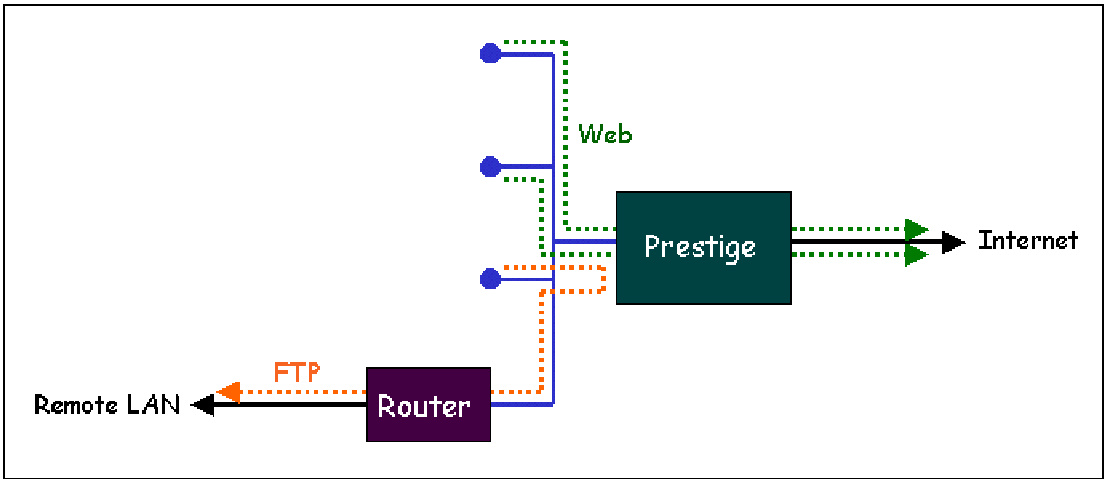
Key Settings:

IP Alias 1	Toggle to **'Yes'** and enter the second LAN IP address for the P-660. This will create the second route in the enif0:0 interface.
IP Alias 2	Toggle to **'Yes'** and enter the third LAN IP address for the P-660. This will create the third route in the enif0:1 interface.

11. Using IP Policy Routing

- What is IP Policy Routing (IPPR)?

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Network administrators can use IPPR to distribute traffic among multiple paths. For example, if a network has both the Internet and remote node connections, we can route the Web packets to the Internet using one policy and route the FTP packets to the remote LAN using another policy. See the figure below.



Use IPPR to distribute traffic among multiple paths

- Benefits

Source-Based Routing - Network administrators can use policy-based routing to direct traffic from different users through different connections.

Quality of Service (QoS)- Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

Cost Savings- IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost path while using low-path for batch traffic.

Load Sharing- Network administrators can use IPPR to distribute traffic among multiple paths.

- How does the IPPR work?

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

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the TOS and precedence fields in the IP header. IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A use defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

- Setup the IP Policy Routing

1. Create a routing policy set in menu 25

```
              Menu 25 - IP Routing Policy Setup
 Policy                          Policy
 Set #     Name                   Set #     Name
 ------  -----------------       ------  -----------------
   1     _________________         7     _________________
   2     _________________         8     _________________
   3     _________________         9     _________________
   4     _________________        10     _________________
   5     _________________        11     _________________
   6     _________________        12     _________________



          Enter Policy Set Number to Configure= 1

          Edit Name= policy1

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

2. Edit a rule or more for this set in menu 25.1.1. See an example below.

```
               Menu 25.1.1 - IP Routing Policy

     Policy Set Name= First
     Active= Yes
     Criteria:
       IP Protocol      = 6
       Type of Service= Don't Care        Packet length= 0
       Precedence       = Don't Care         Len Comp= N/A
       Source:
         addr start= 192.168.1.2          end= 192.168.1.20
         port start= 0                    end= N/A
       Destination:
         addr start= 0.0.0.0              end= N/A
         port start= 80                   end= 80
     Action= Matched
       Gateway addr     = 192.168.1.254       Log= No
       Type of Service= No Change
       Precedence       = No Change

               Press ENTER to Confirm or ESC to Cancel
```

This policy example forces the Web packets originated from the clients with IP addresses from 192.168.1.2 to 192.168.1.20 be routed to the remote LAN via the gateway 192.168.1.254.

4. A summary for this set is shown in menu 25.1.

```
                 Menu 25.1 - IP Routing Policy Setup

# A                        Criteria/Action
- - ------------------------------------------------------------------------
1 Y SA=192.168.1.2-192.168.1.20
    DP=80-80 P=6                              |GW=192.168.1.254
2 N ______________________________________________________________________
    ____________________________________________________________________
3 N ______________________________________________________________________
    ____________________________________________________________________
4 N ______________________________________________________________________
    ____________________________________________________________________
5 N ______________________________________________________________________
    ____________________________________________________________________
6 N ______________________________________________________________________
    ____________________________________________________________________


              Enter Policy Rule Number (1-6) to Configure:
```

4. There are two interfaces to apply the policy set, they are the LAN interface (menu 3.2) and WAN interface (menu 11.3). It depends where the gateway specified in the policy rule is located. If the gateway you specified is located on the local LAN you apply the policy set in menu 3.2 (LAN interface). If the gateway you specified is located on the remote WAN site you apply the policy set in menu 11.3 (WAN interface).

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

   DHCP Setup
      DHCP= Server
      Client IP Pool Starting Address= 192.168.1.33
      Size of Client IP Pool= 32
      Primary DNS Server= 0.0.0.0
      Secondary DNS Server= 0.0.0.0
      Remote DHCP Server= N/A
    TCP/IP Setup:
      IP Address= 192.168.1.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= Both
        Version= RIP-1
      Multicast= None
      IP Policies= 1
      Edit IP Alias= No

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

```
         Menu 11.3 - Remote Node Network Layer Options

   IP Options:                    Bridge Options:
    Rem IP Addr:                     Ethernet Addr Timeout(min)= N/A
    Rem Subnet Mask= 0.0.0.0
    My WAN Addr= 0.0.0.0
    NAT = None
      Address Mapping Set= N/A
```

```
        Metric= 2
        Private= No
        RIP Direction= Both
          Version= RIP-2B
        Multicast= IGMP-v2
        IP Policies= 1


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

12. Using Call Scheduling

- What is Call Scheduling ?

Call scheduling enables the mechanism for the P-660 to run the remote node connection according to the pre-defined schedule. This feature is just like the scheduler ina video recorder which records the program according to the specified time. Users can apply at most 4 schedule sets in Menu 11 (Remote Node Setup), and configure each schedule in Menu 26(Schedule Setup). The remote node configured with the schedule set could be "Forced On", "Forced Down", "Enable Dial-On-Demand", or "Disable Dial-On-Demand" on specified date and time.

- SMT Menu for Call Scheduling

1. Edit the Schedule sets in menu 26:

```


           Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

                      Prestige 660 Main Menu

        Getting Started                Advanced Management
          1. General Setup                21. Filter Set Configuration
          2. WAN Backup Setup             22. SNMP Configuration
          3. LAN Setup                    23. System Password
         4. Internet Access Setup         24. System Maintenance
                                          25. IP Routing Policy Setup
        Advanced Applications             26. Schedule Setup
          11. Remote Node Setup
          12. Static Routing Setup
```

```
     14. Dial-in User Setup        99. Exit
    15. NAT Setup
                   Enter Menu Selection Number:
```

2. Select a Schedule Set number and give it a name:

```
              Menu 26 - Schedule Setup

            Schedule                    Schedule
            Set # Name                    Set # Name
            ------ -----------------    ------ -----------------
            1 ZyXEL                     7 ________________
            2 ________________           8 ________________
            3 ________________           9 ________________
            4 ________________          10 ________________
            5 ________________          11 ________________
            6 ________________          12 ________________

               Enter Schedule Set Number to Configure= 1
               Edit Name= ZyXEL
               Press ENTER to Confirm or ESC to Cancel:
```

3. The Menu 26.1 Schedule Set Setup is as follows:

```
            Menu 26.1 Schedule Set Setup

      Active= Yes
      Start Date(yyyy-mm-dd)= 2002 - 01 - 01
      How Often= Once
      Once:
        Date(yyyy-mm-dd)= 2002 - 01 - 01
      Weekdays:
        Sunday= N/A
        Monday= N/A
        Tuesday= N/A
        Wednesday= N/A
        Thursday= N/A
        Friday= N/A
        Saturday= N/A
      Start Time(hh:mm)= 12 : 00
      Duration(hh:mm)= 16 : 00
```

```
        Action= Enable Dial-on-demand

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

Key Settings:

Start Date	Start date of this schedule rule. It can be unmatched with weekday setting. For example, if Start Date is 2000/10/02(Monday), but Monday setting in weekday can be No.
How Often	If once is selected, all weekday settings will ne marked as N/A. After the rule is completely, it will be deleted automatically.
Forced On	The node will always keep up during the setting period. It is equivalent to diable the idel timeout.
Forced Down	The node will always keep doen during the setting period. The connected remote node will be dropped.
Enable Dial-On-Demand	The remote node accepts Dial-on-demand during this period.
Disable Dial-On-Demand	The remote node denies any demand dial during the period. For the existing connected nodes, it will be dropped after idle timeout and no triggered up.
Start Time/ Duration	Start Time and Duration of this schedule.

- Apply the schedule to the Remote node

Multiple scheduling rules can program in a Remote node, and they have priority. For example, if we program the sets as 1,2,3,4 in remote node, then the set 1 will override set 2,3,4. set 2 will override 3,4, and so on.

```
                        Menu 11.1 - Remote Node Profile

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

     Encapsulation= PPPoE                 Edit IP/Bridge= No
     Multiplexing= LLC-based              Edit ATM Options= No
     Service Name= N/A                    Edit Advance Options= No
     Incoming:                            Telco Option:
       Rem Login= N/A                       Allocated Budget(min)= 0
       Rem Password= N/A                    Period(hr)= 0
     Outgoing:                              Schedule Sets= 1, 2, 3, 4
       My Login= cso@hinet.net              Nailed-Up Connection= No
       My Password= *******               Session Options:
```

```
                Authen= N/A                              Edit Filter Sets= No
                                                        Idle Timeout(sec)= 0
```

- Time Service in P-660

There is no RTC (Real-Time Clock) chip so the P-660 should launch a mechanism to get current time and date from external server in boot time. Time service is implemented by the **Daytime protocol(RFC-867)**, **Time protocol(RFC-868)**, and **NTP protocol(RFC-1305)**. You have to assign an IP address of a time server and then, the P-660 will get the date, time, and time-zone information from this server.

```
    Menu 24.10 - System Maintenance - Time and Date Setting


  Use Time Server when Bootup= Daytime (RFC-867)
  Time Server IP Address= 202.132.154.1

  Current Time: 00 : 11 : 38
  New Time (hh:mm:ss): 00 : 11 : 36

  Current Date: 2000 - 01 - 01
  New Date (yyyy-mm-dd): 2000 - 01 - 01

  Time Zone= GMT+0800

  Daylight Saving= No
  Start Date (mm-dd): 01 - 00
  End Date (mm-dd): 01 - 00


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

13. Using IP Multicast

- What is IP Multicast ?

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. Host groups are identified by class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the P-660 queries all directly connected networks to gather group membership.

After that, the P-660 updates the information by periodic queries. The P-660 implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

- IP Multicast Setup

Enable IGMP in P-660's LAN in menu 3.2:

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

   DHCP Setup
      DHCP= Server
      Client IP Pool Starting Address= 192.168.1.33
      Size of Client IP Pool= 32
      Primary DNS Server= 0.0.0.0
      Secondary DNS Server= 0.0.0.0
      Remote DHCP Server= N/A
    TCP/IP Setup:
      IP Address= 192.168.1.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= Both
        Version= RIP-1
      Multicast= IGMP-v2
      IP Policies=
      Edit IP Alias= No

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

Enable IGMP in P-660's remote node in menu 11.3:

```
         Menu 11.3 - Remote Node Network Layer Options

   IP Options:                    Bridge Options:
    Rem IP Addr:                    Ethernet Addr Timeout(min)= N/A
    Rem Subnet Mask= 0.0.0.0
```

```
My WAN Addr= 0.0.0.0
NAT = None
 Address Mapping Set= N/A
Metric= 2
Private= No
RIP Direction= Both
  Version= RIP-2B
Multicast= IGMP-v2
IP Policies=


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

Key Settings:

Multicast	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2.

14. Using Zero-Configuration

- Zero-Configuration and VC auto-hunting

Zero-Configure feature can help customer to reduce the burden of setting efforts. Whenever system ADSL links up system will send out some probing patterns, system will analyze the packets returned from ISP, and decide which services the ISP may provide. Because ADSL is based on a ATM network, so system have to pre-configured a VPI/VCI hunting pool before Auto-Configure function begins to work.

The Zero-Configuration feature can hunt the encapsulation and VPI/VCI value, and system will automatically configure itself if the hunting result is successfully. This feature has two constraints:

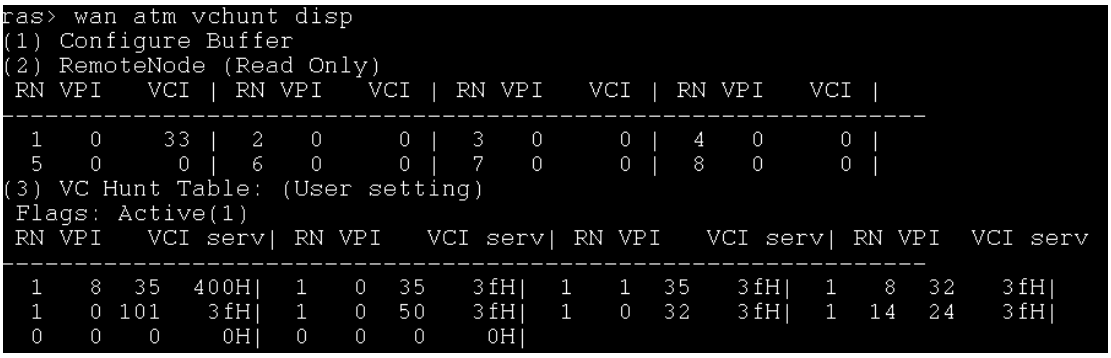
1. It supports the ISP provides one kind of service (PPPoE/PPPoA..etc.) only, otherwise the hunting will get confusing and failed.
2. VC auto-hunting only supports dynamic WAN IP address. If the router is set a static WAN IP address. VC auto-hunting function will be disabled.

The entry of hunting pool must also contain the VPI, VCI, and which kinds of hunting patterns you wish to send. Whenever system send out all the probing patterns with specific VPI/VCI, system will wait for 5~10 seconds and get the response from ISP, the response patterns will decide which kinds of ADSL services of the line will be. After that, system will save back the correct VPI, VCI and also services (encapsulation) type into profile of WAN interface.

- Configure the VC auto-hunting preconfigured table.

1. Display auto-haunting preconfigured table by using CI command from menu 24.8:

```
wan atm vchunt disp
```



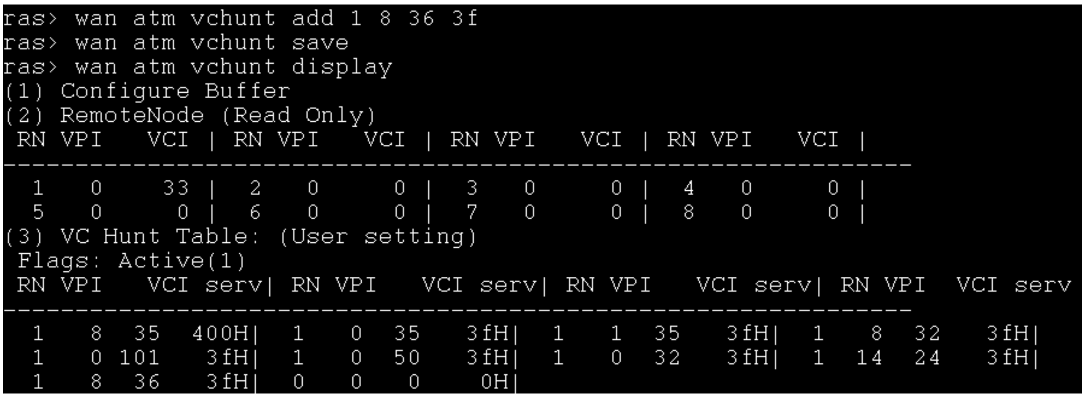
```
ras> wan atm vchunt disp
(1) Configure Buffer
(2) RemoteNode (Read Only)
 RN VPI   VCI | RN VPI   VCI | RN VPI   VCI | RN VPI   VCI |
---------------------------------------------------------------
  1   0    33 |  2   0     0 |  3   0     0 |  4   0     0 |
  5   0     0 |  6   0     0 |  7   0     0 |  8   0     0 |
(3) VC Hunt Table: (User setting)
 Flags: Active(1)
 RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI  VCI serv
---------------------------------------------------------------
  1   8  35  400H|  1   0  35   3fH|  1   1  35   3fH|  1   8  32   3fH|
  1   0 101   3fH|  1   0  50   3fH|  1   0  32   3fH|  1  14  24   3fH|
  0   0   0    0H|  0   0   0    0H|
```

2. Add items to the auto-haunting preconfigured table by useing CI commands:

```
wan atm vchunt add <remoteNodeIndex> <vpi> <vci> <service bit(hex)>
wan atm vchunt save
```

Note: <remote node> : input the remote node index 1-8
<vpi> : vpi value
<vci> : vci value
<service>: it's a hex value, bit0:PPPoE/VC (1), bit1:PPPoE/LLC (2) , bit2:PPPoA/VC (4), bit3:PPPoA/LLC (8), bit4:Enet/VC (16), bit5 :Enet/LLC (32)
For examples:
If you need service PPPoE/LLC and Enet/LLC then the service bits will be 2+32 = 34 (decimal) = 22 (hex), you must input 22
If you want to enable all service for VC hunting, the service bits will be 1+2+4+8+16+32=63(decimal)= 3f (hex), you must input 3f

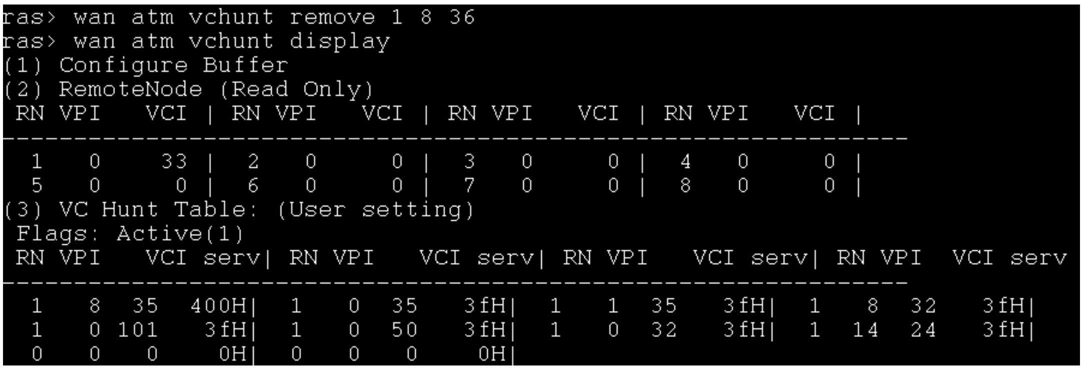
Need to perform save after this command.



```
ras> wan atm vchunt add 1 8 36 3f
ras> wan atm vchunt save
ras> wan atm vchunt display
(1) Configure Buffer
(2) RemoteNode (Read Only)
 RN VPI   VCI | RN VPI   VCI | RN VPI   VCI | RN VPI   VCI |
---------------------------------------------------------------
  1   0    33 |  2   0     0 |  3   0     0 |  4   0     0 |
  5   0     0 |  6   0     0 |  7   0     0 |  8   0     0 |
(3) VC Hunt Table: (User setting)
 Flags: Active(1)
 RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI  VCI serv
---------------------------------------------------------------
  1   8  35   400H|  1   0  35   3fH|  1   1  35   3fH|  1   8  32   3fH|
  1   0 101    3fH|  1   0  50   3fH|  1   0  32   3fH|  1  14  24   3fH|
  1   8  36    3fH|  0   0   0    0H|
```

3. Delete items from the auto-haunting preconfigured table by useing CI command:

wan atm vchunt remove   <remote node> <vpi> <vci>



```
ras> wan atm vchunt remove 1 8 36
ras> wan atm vchunt display
(1) Configure Buffer
(2) RemoteNode (Read Only)
 RN VPI   VCI | RN VPI   VCI | RN VPI   VCI | RN VPI   VCI |
---------------------------------------------------------------
  1   0    33 |  2   0     0 |  3   0     0 |  4   0     0 |
  5   0     0 |  6   0     0 |  7   0     0 |  8   0     0 |
(3) VC Hunt Table: (User setting)
 Flags: Active(1)
 RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI  VCI serv
---------------------------------------------------------------
  1   8  35   400H|  1   0  35   3fH|  1   1  35   3fH|  1   8  32   3fH|
  1   0 101    3fH|  1   0  50   3fH|  1   0  32   3fH|  1  14  24   3fH|
  0   0   0     0H|  0   0   0    0H|
```

5. The usage command argument is listed below suggest to use 3f which include all PPP possiblities.

Command				Description
wan	atm	vchunt		
			Add <remoteNodeIndex> <vpi> <vci> <service bit(hex)>	Add a entry to hunting pool <remote node> : input the remote node index 1-8 <vpi> : vpi value <vci> : vci value <service>: it’s a hex value, bit0:PPPoE/VC (1), bit1:PPPoE/LLC (2) , bit2:PPPoA/VC (4), bit3:PPPoA/LLC (8),

				bit4:Enet/VC (16), bit5 :Enet/LLC (32) For examples: If you need service PPPoE/LLC and Enet/LLC then the service bits will be 2+32 = 34 (decimal) = 22 (hex), you must input 22 Need to perform save after this command
			Remove <removeNodeId> <vpi> <vci>	Input remote node ID and vpi, vci value to remove the specific entry. System will save automatically.
			Active <yes|no>	Enable VC auto hunting featurer
			display	Display the hunt pool
			Clear	Clear the configure buffer
			Save	Save current setting into ROM file
			timer	The waiting time before checking the hunting table result
			Send	Send VC hunt pattern again
			result	Check the result of VC auto hunting

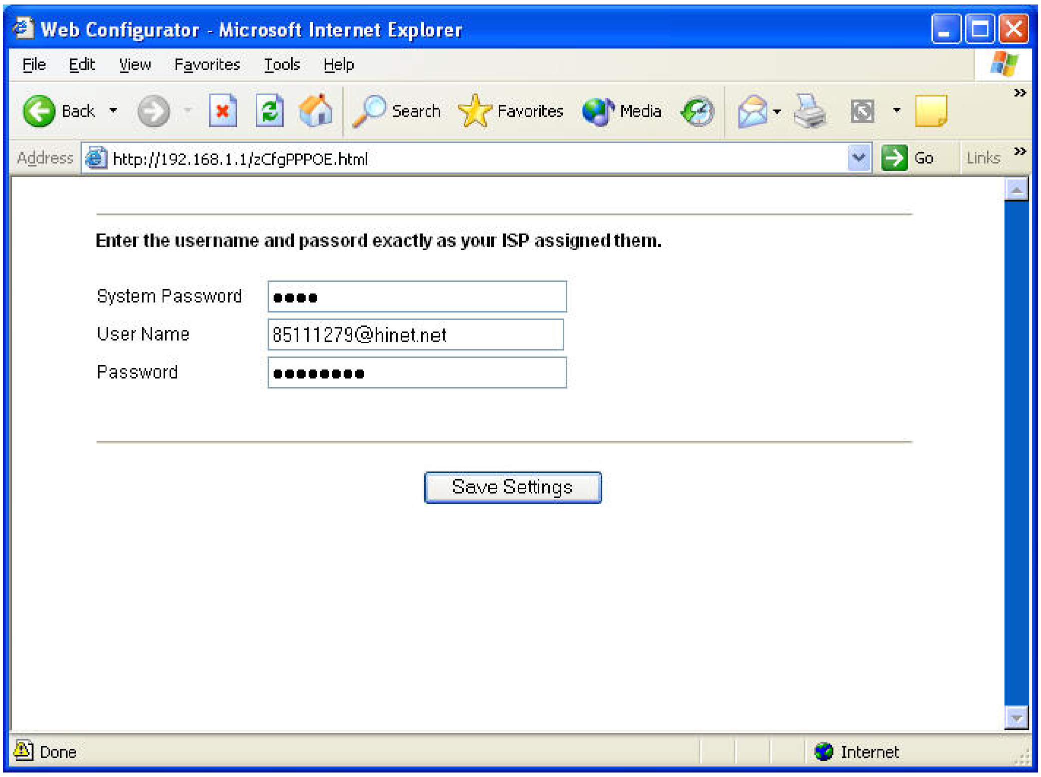
- Using Zero configuration.

1. After configure the auto-haunting preconfigured table. You just need a PC connected to the device LAN Ethernet port with the DSL sync up.

2. Open your web browser to access a Web site. It should prompt and request for your username password of your ISP account, if your ISP provide PPPoE or PPPoA service.

3. After key-in the correct info, it will than test the connection. If it is successful it will than close the browser and you can open a new browser to surf the Internet. If the connection test fail, it will go back to the page ask for user name and password.
The user name or password are incorrect. You need to keyin again to retry.

Basically the zero configuration only work on the VC that was preconigured in the auto-haunting preconfigured table.


Web Configurator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Done
Internet

http://192.168.1.1/zCfgPPPOE.html

Enter the username and passord exactly as your ISP assigned them.

System Password	●●●●
User Name	85111279@hinet.net
Password	●●●●●●●●●

Save Settings

Support Tool

1. LAN/WAN Packet Trace

The Prestige packet trace records and analyzes packets running on LAN and WAN interfaces. It is designed for users with technical backgrounds who are interested in the details of the packet flow on LAN or WAN end of Prestige. It is also very helpful for diagnostics if you have compatibility problems with your ISP or if you want to know the details of a packet for configuring a filter rule.

The format of the display is as following:

Packet:

```
0    11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
```

[index] [timer/second][channel-receive/transmit][length]   [protocol] [sourceIP/port] [destIP/port]

There are two ways to dump the trace:

- **Online Trace**--display the trace real time on screen
- **Offline Trace**--capture the trace first and display later

The details for capturing the trace in SMT menu 24.8 are as follows.

Online Trace

- Trace LAN packet
- Trace WAN packet

1. Trace LAN packet

- Disable to capture the WAN packet by entering: **sys trcp channel mpoa00 none**
- Enable to capture the LAN packet by entering: **sys trcp channel enet0 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Display the brief trace online by entering: **sys trcd brief**
- Display the detailed trace online by entering: **sys trcd parse**

Example:

```
P-660> sys trcp channel mpoa00 none
P-660> sys trcp channel enet0 bothway
P-660> sys trcp sw on
```

```
P-660> sys trcl sw on
P-660> sys trcd brief
   0     11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   1     11883.100 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   2     11883.330 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1108
   3     11883.340 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   4     11883.340 ENET0-R[0339] TCP 192.168.1.2:1108->192.31.7.130:80
   5     11883.610 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   6     11883.620 ENET0-T[0102] TCP 192.31.7.130:80->192.168.1.2:1108
   7     11883.630 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   8     11883.630 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   9     11883.650 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  10     11883.650 ENET0-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80
P-660> sys trcd parse
---<0000>----------------------------------------------------------------
LAN Frame: ENET0-RECV    Size:   62/   62    Time: 12089.790 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

  Ethernet Header:
    Destination MAC Addr      = 00A0C5921311
    Source MAC Addr           = 0080C84CEA63
    Network Type              = 0x0800 (TCP/IP)

  IP Header:
    IP Version                = 4
    Header Length             = 20
    Type of Service           = 0x00 (0)
    Total Length              = 0x0030 (48)
    Idetification             = 0x330B (13067)
    Flags                     = 0x02
    Fragment Offset           = 0x00
    Time to Live              = 0x80 (128)
    Protocol                  = 0x06 (TCP)
    Header Checksum           = 0x3E71 (15985)
    Source IP                 = 0xC0A80102 (192.168.1.2)
    Destination IP            = 0xC01F0782 (192.31.7.130)

  TCP Header:
    Source Port               = 0x045C (1116)
    Destination Port          = 0x0050 (80)
    Sequence Number           = 0x00BD15A7 (12391847)
    Ack Number                = 0x00000000 (0)
    Header Length             = 28
    Flags                     = 0x02 (....S.)
    Window Size              = 0x2000 (8192)
    Checksum                 = 0xBEC3 (48835)
    Urgent Ptr               = 0x0000 (0)
    Options                  =
      0000: 02 04 05 B4 01 01 04 02

  RAW DATA:
  0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00   .........L.c..E.
  0010: 00 30 33 0B 40 00 80 06-3E 71 C0 A8 01 02 C0 1F   .03.@...>q......
  0020: 07 82 04 5C 00 50 00 BD-15 A7 00 00 00 00 70 02   ...\.P........p.
  0030: 20 00 BE C3 00 00 02 04-05 B4 01 01 04 02         .............
---<0001>------------------------------------------------------------------
LAN Frame: ENET0-XMIT    Size:   58/   58    Time: 12090.020 sec
Frame Type: TCP 192.31.7.130:80->192.168.1.2:1116

  Ethernet Header:
    Destination MAC Addr     = 0080C84CEA63
    Source MAC Addr          = 00A0C5921311
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x002C (44)
    Idetification            = 0x57F3 (22515)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0xED (237)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0xAC8C (44172)
    Source IP                = 0xC01F0782 (192.31.7.130)
    Destination IP           = 0xC0A80102 (192.168.1.2)

  TCP Header:
    Source Port              = 0x0050 (80)
    Destination Port         = 0x045C (1116)
    Sequence Number          = 0x4AD1B57F (1255257471)
    Ack Number               = 0x00BD15A8 (12391848)
    Header Length            = 24
    Flags                    = 0x12 (.A..S.)
    Window Size              = 0xFAF0 (66040)
    Checksum                 = 0xF877 (63607)
    Urgent Ptr               = 0x0000 (0)
    Options                =
        0000: 02 04 05 B4

  RAW DATA:
  0000: 00 80 C8 4C EA 63 00 A0-C5 92 13 11 08 00 45 00   ...L.c........E.
  0010: 00 2C 57 F3 40 00 ED 06-AC 8C C0 1F 07 82 C0 A8   .,W.@..........
  0020: 01 02 00 50 04 5C 4A D1-B5 7F 00 BD 15 A8 60 12   ...P.\J.......`.
  0030: FA F0 F8 77 00 00 02 04-05 B4                     ...w......
---<0002>---------------------------------------------------------------
LAN Frame: ENET0-RECV    Size:   60/   60    Time: 12090.210 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

  Ethernet Header:
    Destination MAC Addr     = 00A0C5921311
    Source MAC Addr          = 0080C84CEA63
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x0028 (40)
    Idetification            = 0x350B (13579)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0x80 (128)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0x3C79 (15481)
    Source IP                = 0xC0A80102 (192.168.1.2)
    Destination IP           = 0xC01F0782 (192.31.7.130)

  TCP Header:
    Source Port              = 0x045C (1116)
    Destination Port         = 0x0050 (80)
    Sequence Number          = 0x00BD15A8 (12391848)
    Ack Number               = 0x4AD1B580 (1255257472)
    Header Length            = 20
    Flags                    = 0x10 (.A....)
    Window Size              = 0x2238 (8760)
    Checksum                 = 0xE8ED (59629)
    Urgent Ptr               = 0x0000 (0)

  TCP Data: (Length=6, Captured=6)
```

```
   0000: 20 20 20 20 20 20

 RAW DATA:
 0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00   .........L.c..E.
 0010: 00 28 35 0B 40 00 80 06-3C 79 C0 A8 01 02 C0 1F   .(5.@...<y......
 0020: 07 82 04 5C 00 50 00 BD-15 A8 4A D1 B5 80 50 10   ...\.P....J...P.
 0030: 22 38 E8 ED 00 00 20 20-20 20 20 20               "8....
```

2. Trace WAN packet

- Disable the capture of the LAN packet by entering: **sys trcp channel enet0 none**
- Enable to capture the WAN packet by entering: **sys trcp channel mpoa00 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Display the brief trace online by entering: **sys trcd brief**
- Display the detailed trace online by entering: **sys trcd parse**

Example:

```
P-660> sys trcp channel enet0 none
P-660> sys trcp channel mpoa00 bothway
P-660> sys trcp sw on
P-660> sys trcl sw on
P-660> sys trcd brief
0     12367.680 MPOA00-R[0070] UDP 202.132.155.95:520->202.132.155.255:520
1     12370.980 MPOA00-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
P-660> sys trcd parse
---<0000>----------------------------------------------------------------
LAN Frame: MPOA00-RECV    Size:1181/   96    Time: 12387.260 sec
Frame Type: TCP 192.31.7.130:80->202.132.155.97:10270

  Ethernet Header:
    Destination MAC Addr      = 00A0C5921312
    Source MAC Addr           = 00A0C5012345
    Network Type              = 0x0800 (TCP/IP)

  IP Header:
    IP Version                = 4
    Header Length             = 20
    Type of Service           = 0x00 (0)
    Total Length              = 0x048B (1163)
    Idetification             = 0xB139 (45369)
    Flags                     = 0x02
    Fragment Offset           = 0x00
    Time to Live              = 0xEE (238)
    Protocol               = 0x06 (TCP)
    Header Checksum        = 0xA9AB (43435)
    Source IP              = 0xC01F0782 (192.31.7.130)
    Destination IP         = 0xCA849B61 (202.132.155.97)

  TCP Header:
    Source Port            = 0x0050 (80)
    Destination Port       = 0x281E (10270)
    Sequence Number        = 0xD3E95985 (3555285381)
    Ack Number             = 0x00C18F63 (12685155)
    Header Length          = 20
    Flags                  = 0x19 (.AP..F)
    Window Size            = 0xFAF0 (66040)
    Checksum               = 0x3735 (14133)
    Urgent Ptr             = 0x0000 (0)

  TCP Data: (Length=1127, Captured=42)
  0000: DF 33 AF 62 58 37 52 3D-79 99 A5 3C 2B 59 E2 78   .3.bX7R=y..<+Y.x
  0010: A7 98 8F 3F A9 09 E4 0F-26 14 9C 58 3E 95 3E E7   ...?....&..X>.>.
  0020: FC 2A 4C 2F FB BE 2F FE-EF D0                     .*L/../...

  RAW DATA:
  0000: 00 A0 C5 92 13 12 00 A0-C5 01 23 45 08 00 45 00   ..........#E..E.
  0010: 04 8B B1 39 40 00 EE 06-A9 AB C0 1F 07 82 CA 84   ...9@..........
  0020: 9B 61 00 50 28 1E D3 E9-59 85 00 C1 8F 63 50 19   .a.P(...Y....cP.
  0030: FA F0 37 35 00 00 DF 33-AF 62 58 37 52 3D 79 99   ..75...3.bX7R=y.
  0040: A5 3C 2B 59 E2 78 A7 98-8F 3F A9 09 E4 0F 26 14   .<+Y.x...?....&.
  0050: 9C 58 3E 95 3E E7 FC 2A-4C 2F FB BE 2F FE EF D0   .X>.>..*L/../...
```

Offline Trace

- Disable the capture of the WAN packet by entering: **sys trcp channel mpoa00 none**
- Enable the capture of the LAN packet by entering: **sys trcp channel enet0 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Wait for packet passing through the Prestige over LAN
- Disable the trace log by entering: **sys trcp sw off** & **sys trcl sw off**
- Display the trace briefly by entering: **sys trcp brief**
- Display specific packets by using: **sys trcp parse <from_index> <to_index>**

2. Firmware/Configurations Uploading and Downloading using TFTP

- Using TFTP client software
- Using TFTP command on Windows NT
- Using TFTP command on UNIX

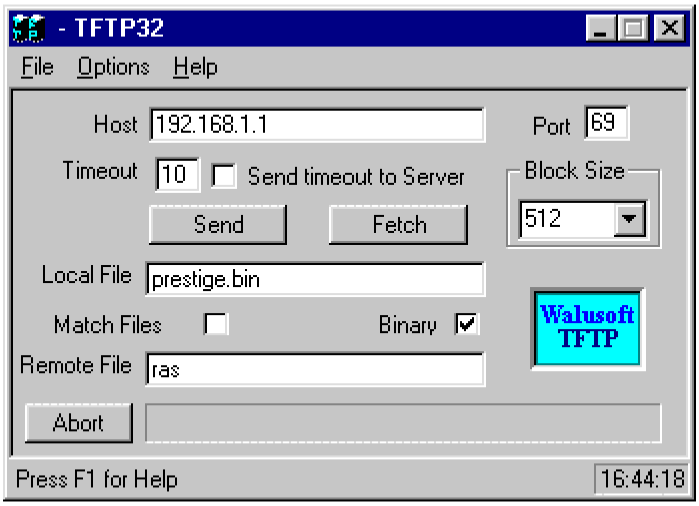
Using TFTP client software

- Upload/download ZyNOS via LAN
- Upload/download SMT configurations via LAN

Using TFTP to upload/download ZyNOS via LAN

- TELNET to your Prestige first before running the TFTP software
- Type the CI command **'sys stdio 0'** to disable console idle timeout in Menu 24.8 and stay in Menu 24.8
- Run the TFTP client software
- Enter the IP address of the Prestige
- To upload the firmware, please save the remote file as **'ras'** to Prestige. After the transfer is complete, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.

An example:



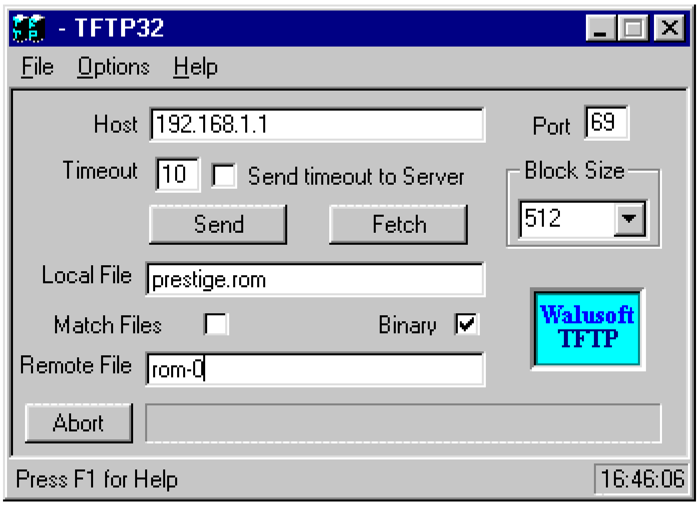
Host: 192.168.1.1
Port: 69
Timeout: 10
□ Send timeout to Server
Block Size: 512
Local File: prestige.bin
Match Files □
Binary ☑
Remote File: ras

The 192.168.1.1 is the IP address of the Prestige. The local file is the source file of the ZyNOS firmware that is available in your hard disk. The remote file is the file name that will be saved in Prestige. Check the port number 69 and 512-Octet blocks for TFTP. Check **'Binary'** mode for file transfering.

Using TFTP to upload/download SMT configurations via LAN

- TELNET to your Prestige first before running the TFTP software
- Type the CI command **'sys stdio 0'** to disable console idle timeout in Menu 24.8 and stay in Menu 24.8
- Run the TFTP client software
- To download the SMT configuration, please get the remote file **'rom-0'** from the Prestige.
- To upload the SMT configuration, please save the remote file as **'rom-0'** in the Prestige.

An example:



Host 192.168.1.1
Port 69
Timeout 10
□ Send timeout to Server
Block Size 512
Local File prestige.rom
Match Files □
Binary ☑
Remote File rom-0
Press F1 for Help
16:46:06

- The 192.168.1.1 is the IP address of the Prestige.
- The local file is the source file of your configuration file that is available in your hard disk.
- The remote file is the file name that will be saved in Prestige.
- Check the port number 69 and 512-Octet blocks for TFTP.
- Check 'Binary' mode for file transfering.

Using TFTP command on Windows NT

Before you begin:

1. TELNET to your Prestige first before using TFTP command
2. Type the CI command **'sys stdio 0'** to disable console idle timeout in Menu 24.8 and stay in Menu 24.8

- **Download ZyNOS via LAN**

```
c:\tftp -i [PrestigeIP] get ras [localfile]
```

- **Upload SMT configurations via LAN**

```
c:\tftp -i [PrestigeIP] put [localfile] rom-0
```

- **Download SMT configurations via LAN**

```
c:\tftp -i [PrestigeIP] get rom-0 [localfile]
```

Using TFTP command on UNIX

Before you begin:

1. TELNET to your Prestige first before using TFTP command
2. Type the CI command **'sys stdio 0'** to disable console idle timeout in Menu 24.8 and stay in Menu 24.8

Example:

```
[cppwu@faelinux cppwu]$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Password: ****
              Copyright (c) 1994 – 2005 ZyXEL Communications Corp.
                      Prestige 660 Main Menu
     Getting Started                   Advanced Management
     1. General Setup                   21. Filter Set Configuration
     3. Ethernet Setup                  22. SNMP Configuration
     4. Internet Access Setup           23. System Password
                                        24. System Maintenance
    Advanced Applications
     11. Remote Node Setup
     12. Static Routing Setup
     15. SUA Server Setup                  99. Exit



                   Enter Menu Selection Number: 24
```

```
          Menu 24 - System Maintenance

               1.  System Status
               2.  System Information and Console Port Speed
               3.  Log and Trace
               4.  Diagnostic
               5.  Backup Configuration
               6.  Restore Configuration
               7.  Firmware Update
               8.  Command Interpreter Mode

          Enter Menu Selection Number: 8

Copyright (c) 1994-2005   ZyXEL Communications Corp.
ras> sys stdio 0
(Open a new window)
[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 get rom-0 [local-rom] <- change to binary mode

<- download configurations

[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 put [local-rom] rom-0 <- upload configurations

[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 get ras [local-ras ] <- download firmware

[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 put [local-ras] ras <- upload firmware
```

3. Using FTP to Upload the Firmware and Configuration Files

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

To use this feature, your workstation must have a FTP client software. There are two examples as shown below.

- Using FTP command in terminal
- Using FTP client software

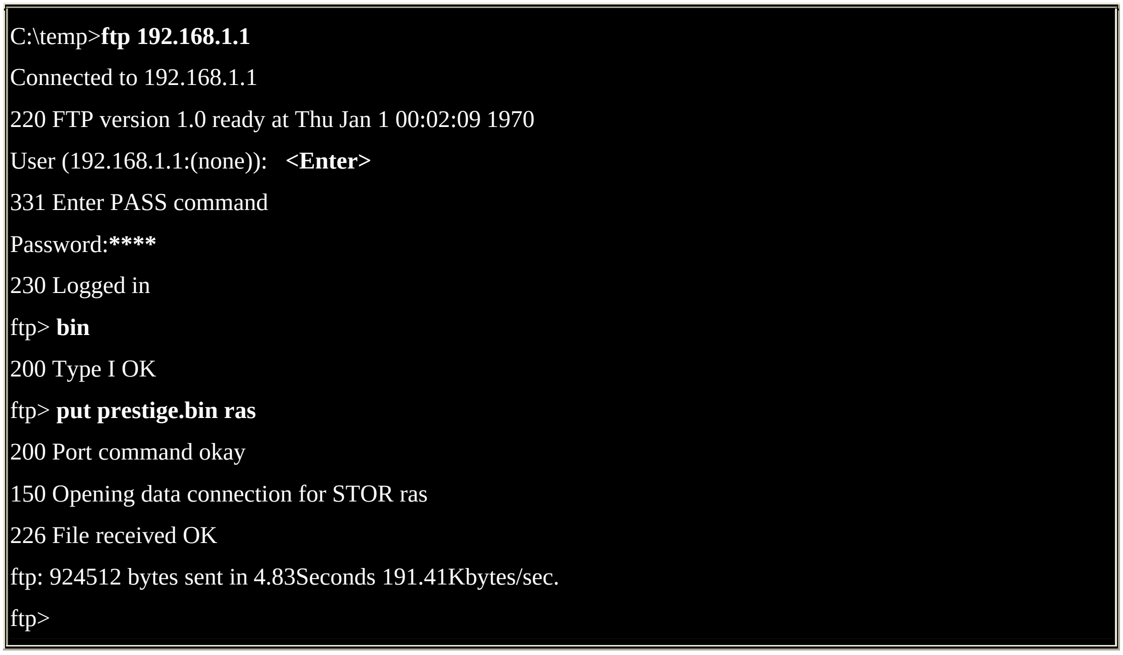
Using FTP command in terminal

Step 1	Use FTP client from your workstation to connect to the Prestige by entering

	the IP address of the Prestige.
Step2	Press **'Enter'** key to ignore the username, because the Prestige does not check the username.
Step 3	Enter the SMT password as the FTP login password, the default is **'1234**'.
Step 4	Enter command **'bin'** to set the transfer type to binary.
Step 5	Use **'put'** command to transfer the file to the Prestige.

Note: The remote file name for the firmware is **'ras'** and for the configuration file is **'rom-0'** (rom-zero, not capital o).

Example:



```
C:\temp>ftp 192.168.1.1
Connected to 192.168.1.1
220 FTP version 1.0 ready at Thu Jan 1 00:02:09 1970
User (192.168.1.1:(none)):   <Enter>
331 Enter PASS command
Password:****
230 Logged in
ftp> bin
200 Type I OK
ftp> put prestige.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 924512 bytes sent in 4.83Seconds 191.41Kbytes/sec.
ftp>
```

Here, the **'prestige.bin'** is the local file and **'ras'** is the remote file that will be saved in the Prestige.

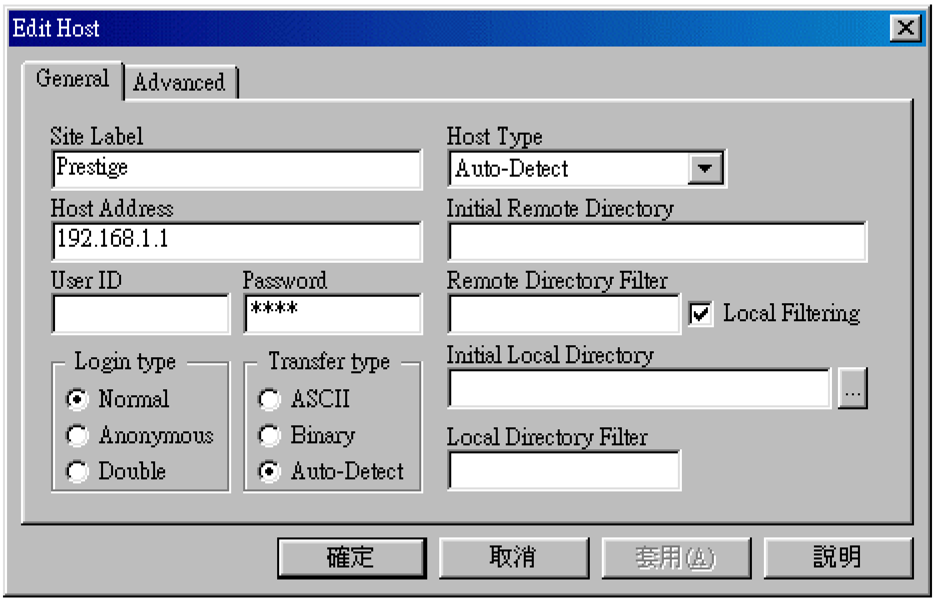
The Prestige reboots automatically after the uploading is finished.

Using FTP client software

Step 1	Rename the local firmware and configuration files to **'ras'** and **'rom-0'**, because we can not specify the remote file name in the FTP client software.
Step 2	Use FTP client from your workstation to connect to the Prestige by entering the IP address of the Prestige.
Step 3	Enter the SMT password as the FTP login password. The default is **'1234'**.
Step 4	Press **'OK'** key to ignore the username, because the Prestige does not check the username.

Example:

1. Connect to the Prestige by entering the Prestige's IP and SMT password in the FTP software. Set the transfer type to '**Auto-Detect**' or '**Binary**'.



Edit Host

Site Label: Prestige

Host Type: Auto-Detect

Host Address: 192.168.1.1

Initial Remote Directory:

User ID:

Password: ****

Remote Directory Filter:

☑ Local Filtering

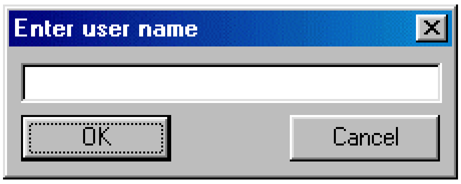
Initial Local Directory:

Local Directory Filter:

Login type: ● Normal ○ Anonymous ○ Double

Transfer type: ○ ASCII ○ Binary ● Auto-Detect

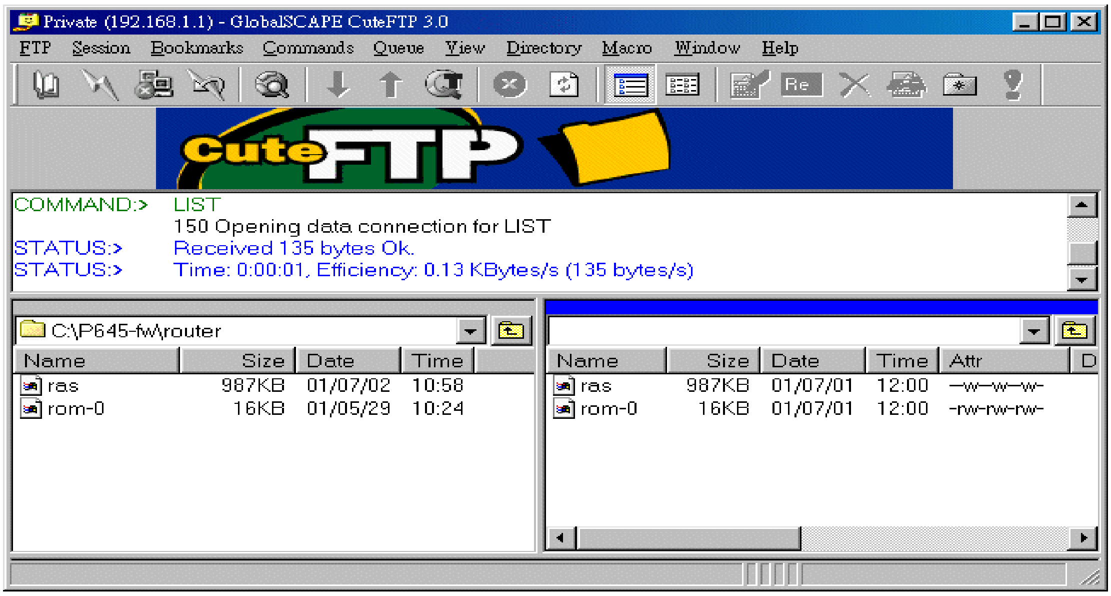
2. Press '**OK**' to ignore the 'Username' prompt.



Enter user name

3. To upload the firmware file, we transfer the local '**ras**' file to overwrite the remote '**ras**' file.

To upload the configuration file, we transfer the local '**rom-0**' to overwrite the remote **'rom-0'** file.


Private (192.168.1.1) - GlobalSCAPE CuteFTP 3.0
FTP Session Bookmarks Commands Queue View Directory Macro Window Help
CuteFTP

```
COMMAND:>   LIST
            150 Opening data connection for LIST
STATUS:>    Received 135 bytes Ok.
STATUS:>    Time: 0:00:01, Efficiency: 0.13 KBytes/s (135 bytes/s)
```

C:\P645-fw\router

Name	Size	Date	Time
ras	987KB	01/07/02	10:58
rom-0	16KB	01/05/29	10:24

Name	Size	Date	Time	Attr	D
ras	987KB	01/07/01	12:00	-w--w--w-	
rom-0	16KB	01/07/01	12:00	-rw-rw-rw-	

4. The Prestige reboots automatically after the uploading is finished. Please do not power off the router at this moment.

CI Command Reference

Command Syntax and General User Interface

CI has the following command syntax:

command <*iface* | *device* > **subcommand** [*param*]
command subcommand [*param*]
command ? | help
command subcommand ? | help

General user interface:

1.	**?**	Shows the following commands and all major (sub)commands
2.	**exit**	Returns to SMT

To get the latest CI Command list

The latest CI Command list is available in release note of every ZyXEL firmware release. Please goto ZyXEL public WEB site http://www.zyxel.com/support/download_index.php to download firmware package (*.zip), you should unzip the package to get the release note in PDF format.