P-2302HW SERIES

VoIP Station Gateway

(With Lifeline/ DECT/ USB)

Support Notes

Version 3.60

Aug. 2006

ZyXEL

Unleash Networking Power

INDEX

Application Notes

General Application Notes

Internet Connection

The following figure shows a typical Internet access application using the Prestige. Before accessing the Internet in an office environment, you must configure the Prestige as outlined below.

- Before you begin
- Setting up Your Windows Computer
- Setting up the Prestige router
- Troubleshooting

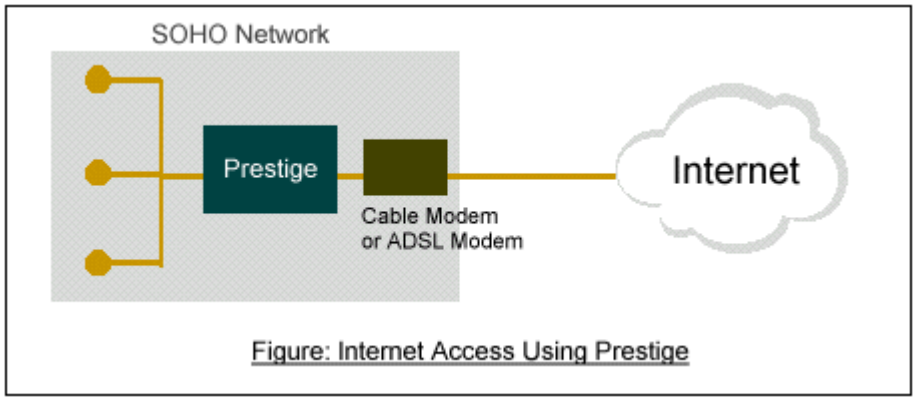


Figure: Internet Access Using Prestige

- Before you begin

The following lists the default settings on the Prestige.

1. IP address = 192.168.1.1, subnet mask = 255.255.255.0 (24 bits)
2. DHCP server enabled with IP pool starting from 192.168.1.33
3. Default SMT menu password = 1234

- Setting up your Windows computer(s)

1. Ethernet connection

Your computer(s) must have an Ethernet card installed.

- If you have only one computer, connect the computer to the LAN port on the Prestige using a crossover Ethernet cable (red).
- If you have more than one computer, you must use a hub or switch to connect the computers to the LAN port on the Prestige using a straight-though Ethernet cable.

2. TCP/IP Installation

You must first install TCP/IP software on each computer before you can use it for Internet access. If you have already installed TCP/IP, go to the next section to configure it; otherwise, follow these steps to install the software:

- In the **Control Panel/Network** window, click **Add** button.
- In the **Select Network Component Type** window, select **Protocol** and click **Add**.
- In the **Select Network Protocol** window, select **Microsoft** and then select **TCP/IP** from the **Network Protocols** field and click **OK**.

3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

- In the **Control Panel/Network** window, select **TCP/IP** and click **Properties**.
- In the **TCP/IP** Properties window, select **obtain an IP address automatically**.

Note: Do not assign arbitrary IP address and subnet mask to your computer(s). Otherwise, you will not be able to access the Internet.

- Click the **WINS** configuration tab and select **Disable WINS Resolution**.
- Click the **Gateway** tab. Select any installed gateways and click the **Remove** button until there is none listed.
- Click the **DNS Configuration** tab and select **Disable DNS**.
- Click **OK** to save and close the **TCP/IP** properties window
- Click **OK** to close the Network window. You will be prompted to insert your Windows CD or disk. When the drivers are updated, you will be asked if you want to restart the computer. Make sure your Prestige is turned on before clicking **Yes**. Repeat the above steps for each Windows computer on your network.

- **Setting up the Prestige router**

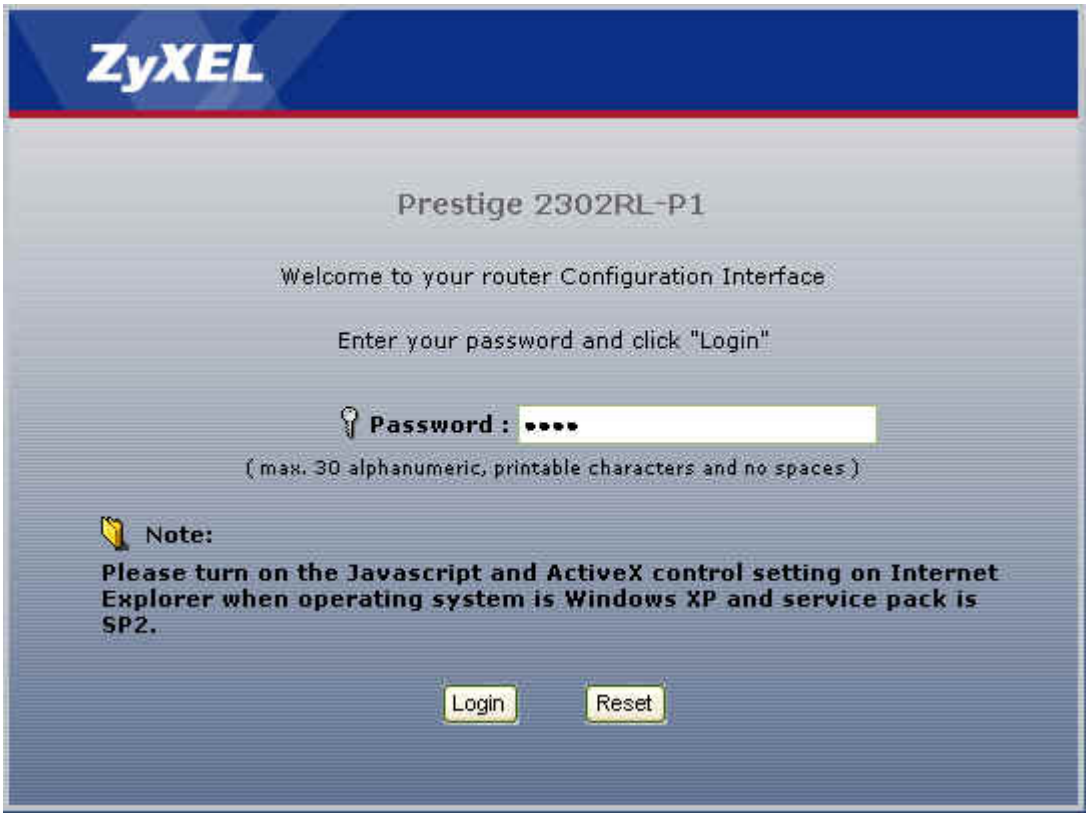
If you have a Single User Account (SUA), follow the procedure to configure the Prestige. You can use a web browser (such as IE) to access the embedded web server on the Prestige for device management. Before you can log into the web management interface, make sure that there is no one logging into the Prestige through Telnet or the console port.

1. Accessing the Prestige Web Management Interface

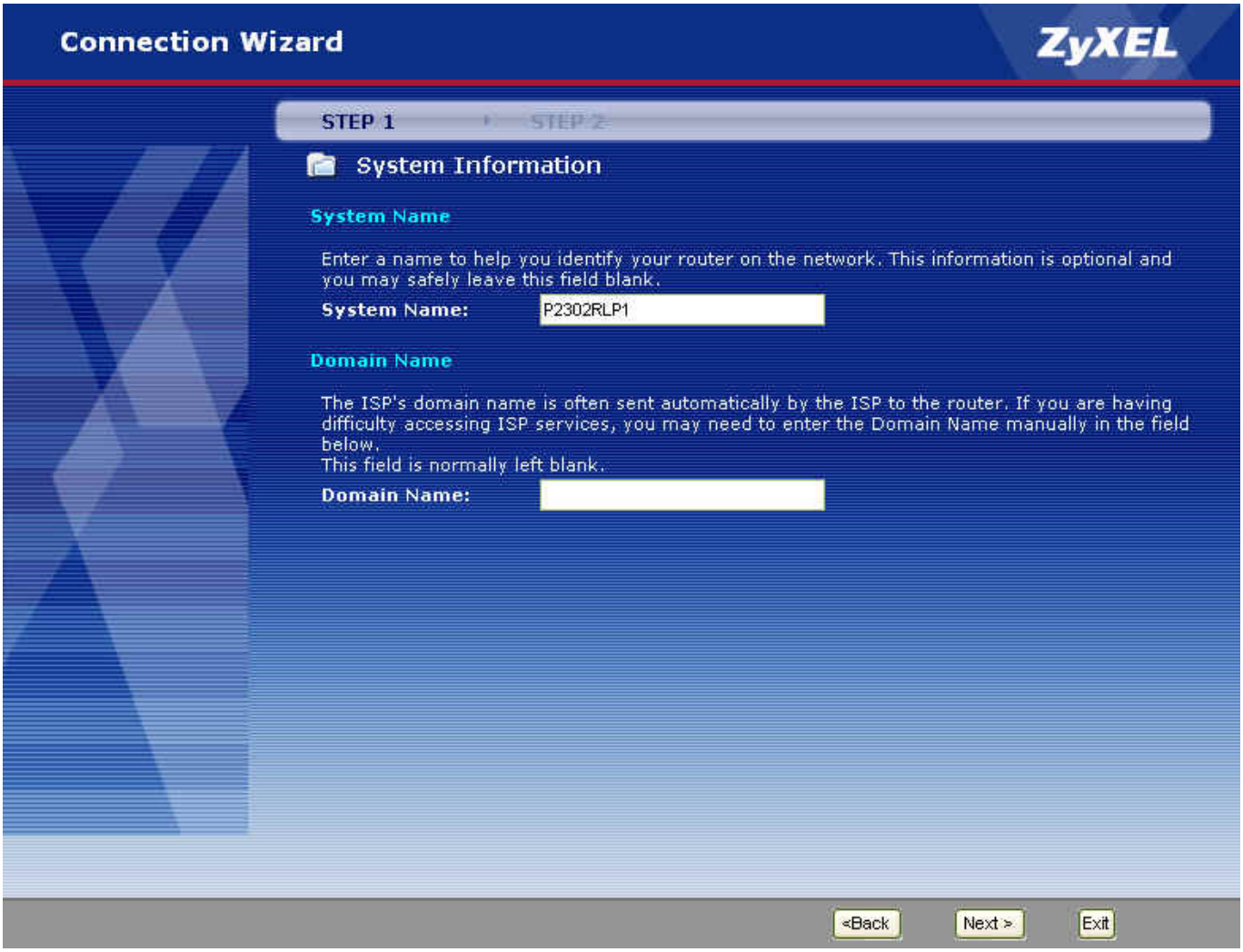
Open your web browser (such as IE) and enter the LAN IP address of the Prestige in the Address field. The default LAN IP of the Prestige is 192.168.1.1. Note that you can either enter http://192.168.1.1 or https://192.168.1.1 (for secure login).

2. First Login

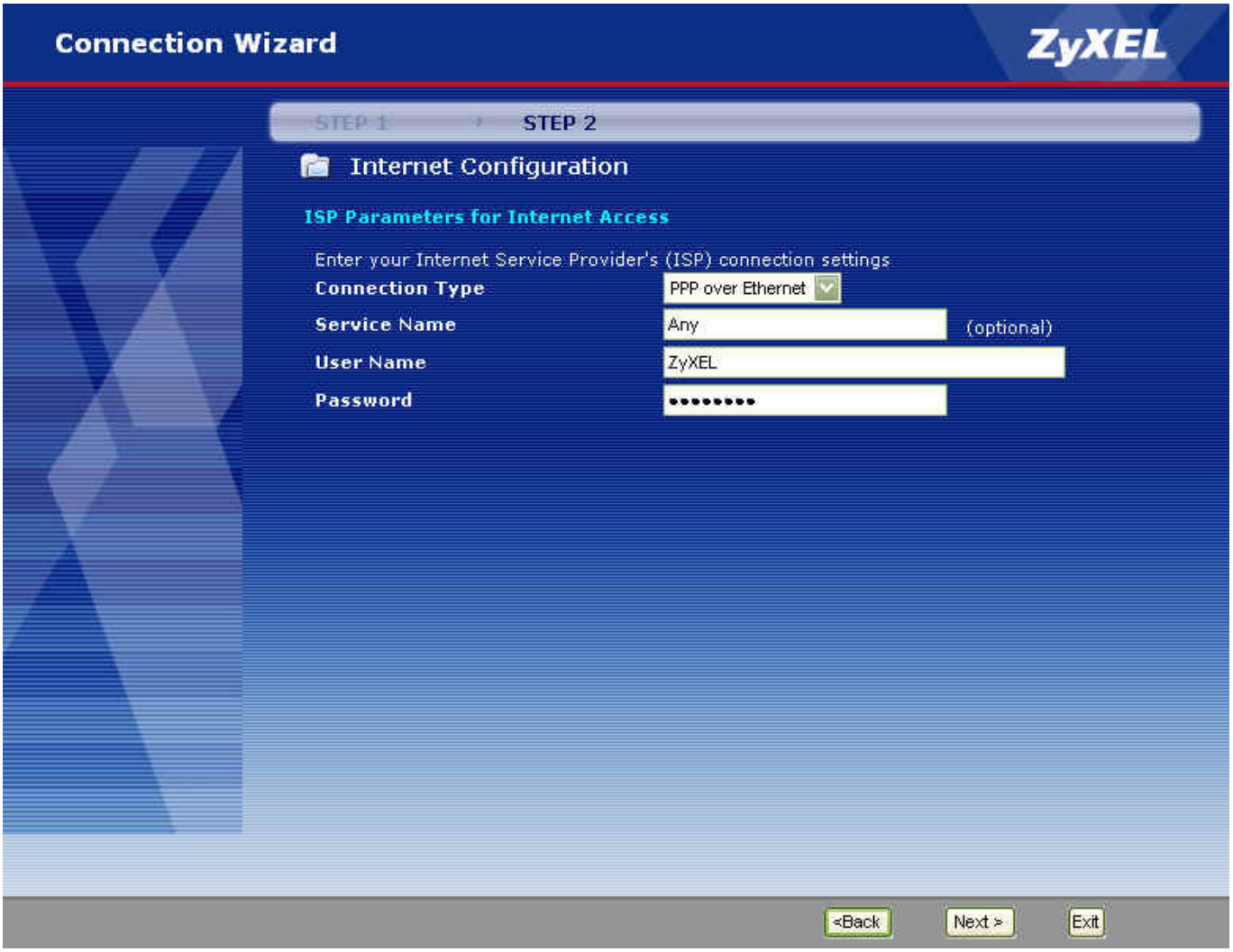
A login screen displays. Enter the password and press Login. The default password is '1234' which is the same as the one you use to log into the SMT.



3. Use the WIZARD SETUP screens to configure Internet access settings on the Prestige.

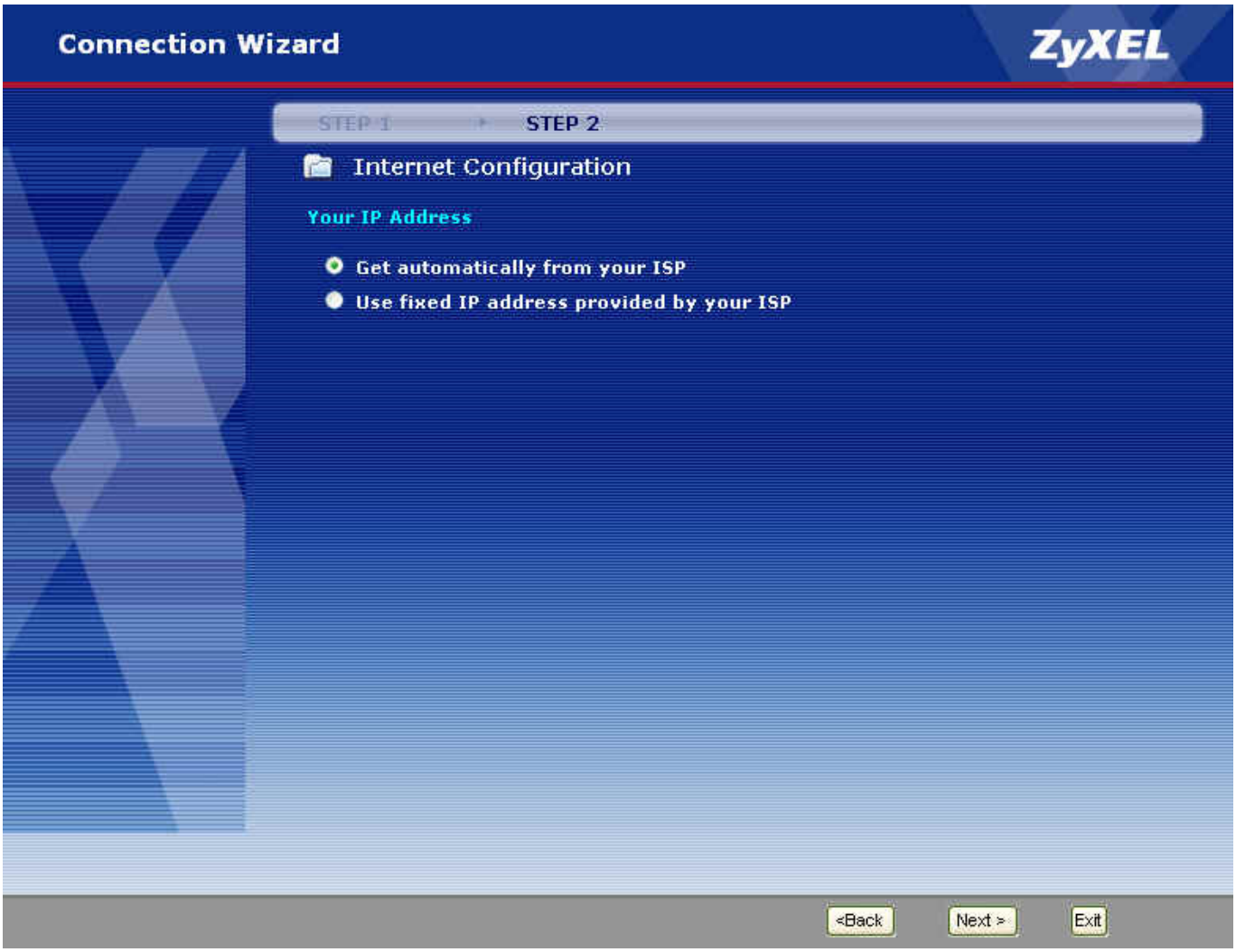


The Internet access configuration screen varies depending on the Internet connection type you select. The following figure shows an example screen for PPPoE connection type.



In the next wizard screen, select **Get dynamically from your ISP** if the ISP assigns you an IP address dynamically, otherwise select **Use Fixed IP address** and enter the static IP address given by ISP in the **MY**

WAN IP Address field.



Setup the Prestige as a DHCP Relay

- What is DHCP Relay?

DHCP (Dynamic Host Configuration Protocol) allows a network device to obtain IP settings from a server. You can configure the P-2602 as a DHCP server or DHCP relay.

When the P-2602 is configured as a DHCP server, it assigns IP address to clients on the LAN. When the P-2602 acts as a DHCP relay, it forwards client DHCP requests to the DHCP server and forwards the responds from the DHCP server to the DHCP clients. The following figure shows an example.

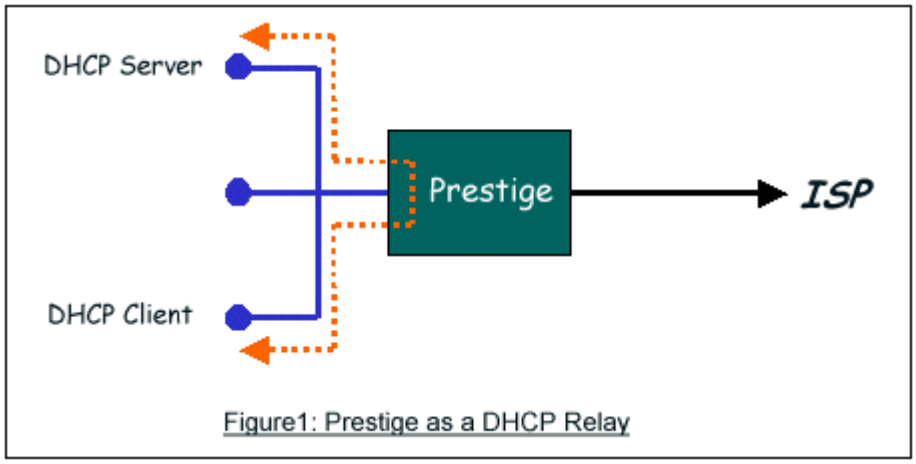


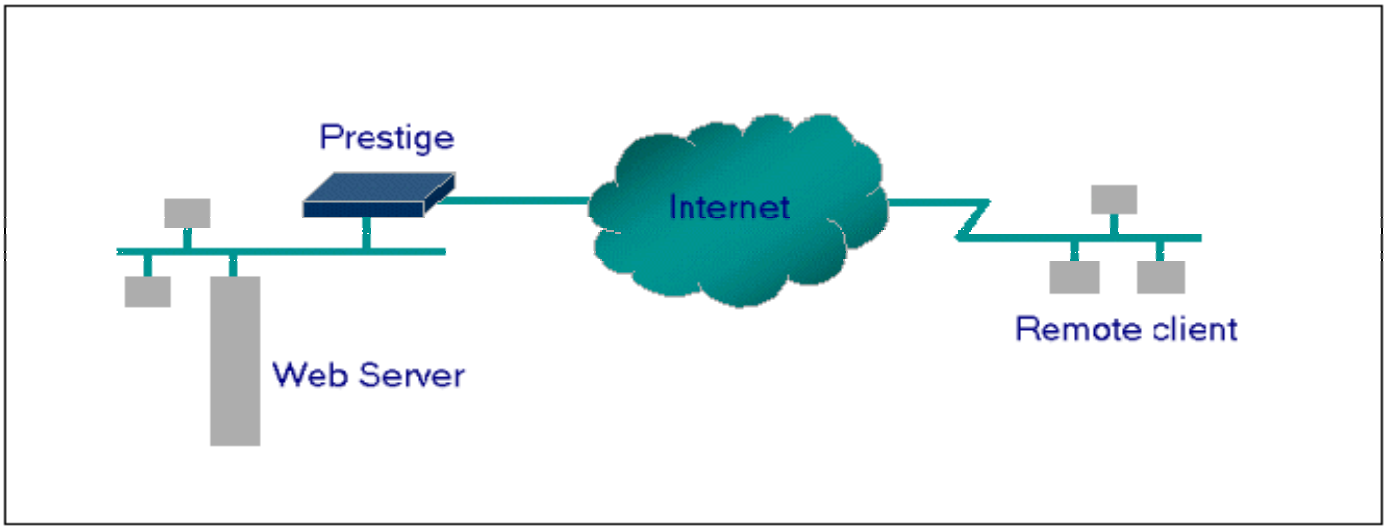
Figure1: Prestige as a DHCP Relay

- Setup the Prestige as a DHCP Client

1. In SMT menu 3.2, select **Relay** in the **DHCP** field and enter the IP address of the DHCP server in the **DHCP Server Address** field.

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

DHCP= Relay                          TCP/IP Setup:
Client IP Pool:
  Starting Address= N/A              IP Address= 192.168.1.1
  Size of Client IP Pool= N/A        IP Subnet Mask= 255.255.255.0
First DNS Server= N/A                RIP Direction= Both
  IP Address= N/A                      Version= RIP-1
Second DNS Server= N/A               Multicast= None
  IP Address= N/A                    Edit IP Alias= No
Third DNS Server= N/A
  IP Address= N/A
DHCP Server Address= 192.168.1.2

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

Configure an Internal Server Behind the Prestige



- Introduction

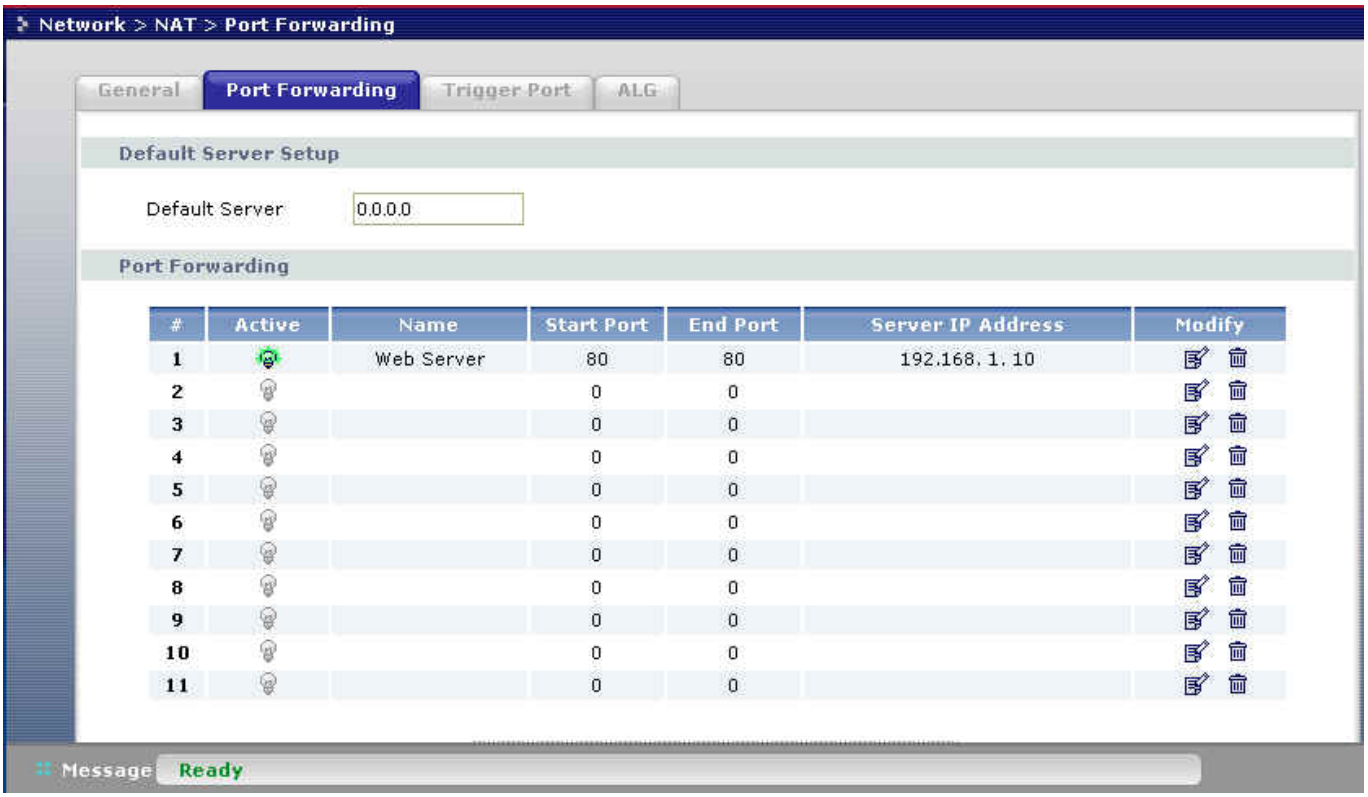
SUA makes your LAN appear as a single machine to the outside world. However, you can make a server (such as a web server, FTP server or mail server) behind the ZyXEL device assessable/visible to the outside world. A server behind the ZyXEL device cannot be set to be a DHCP client. That is, the server must use a fixed IP address so outside users can access the server using the static IP address.

A service is identified by its standard port number. You can allow public access to servers for specified services based on the port number. In addition, you can also set a default server behind SUA. Thus service requests that do not match any of the servers are forwarded to the default server. If you do not set a default SUA server, then the unknown service requests are simply discarded.

- Configuration

To make an inside server visible to the outside world, specify the service port number and the IP address of the server in SMT menu 15.2.1 - NAT Server Setup or the Port Forwarding screen in the web configurator. Users use the WAN IP address of the Prestige to access the inside SUA servers. You can obtain the WAN IP address of the Prestige in SMT menu 24.1.

- The following figure shows a configuration example to allow public access to an internal Web server.



- The following table lists some common service port numbers.

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

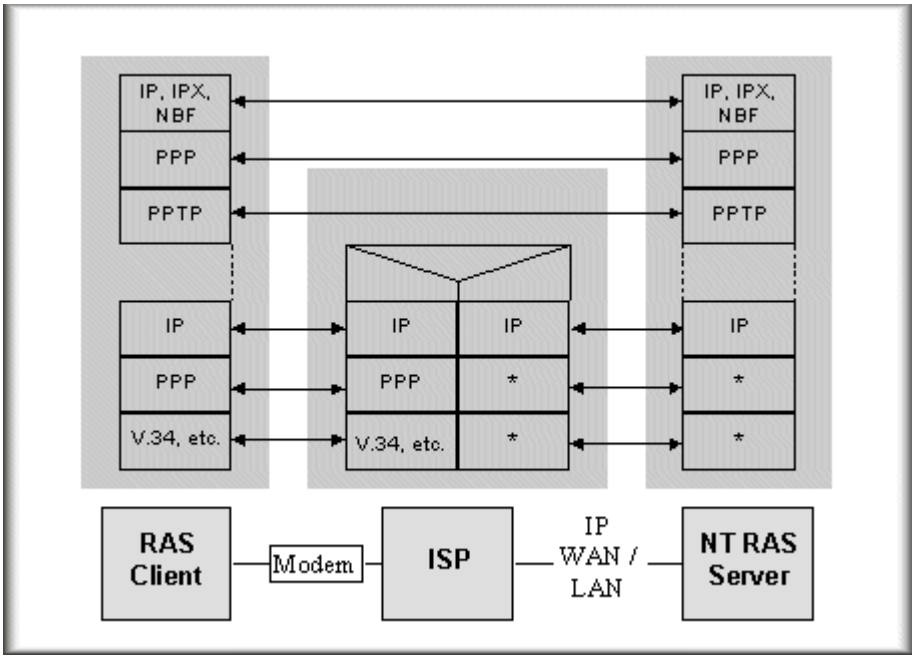
Configure a PPTP server Behind SUA

- 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.



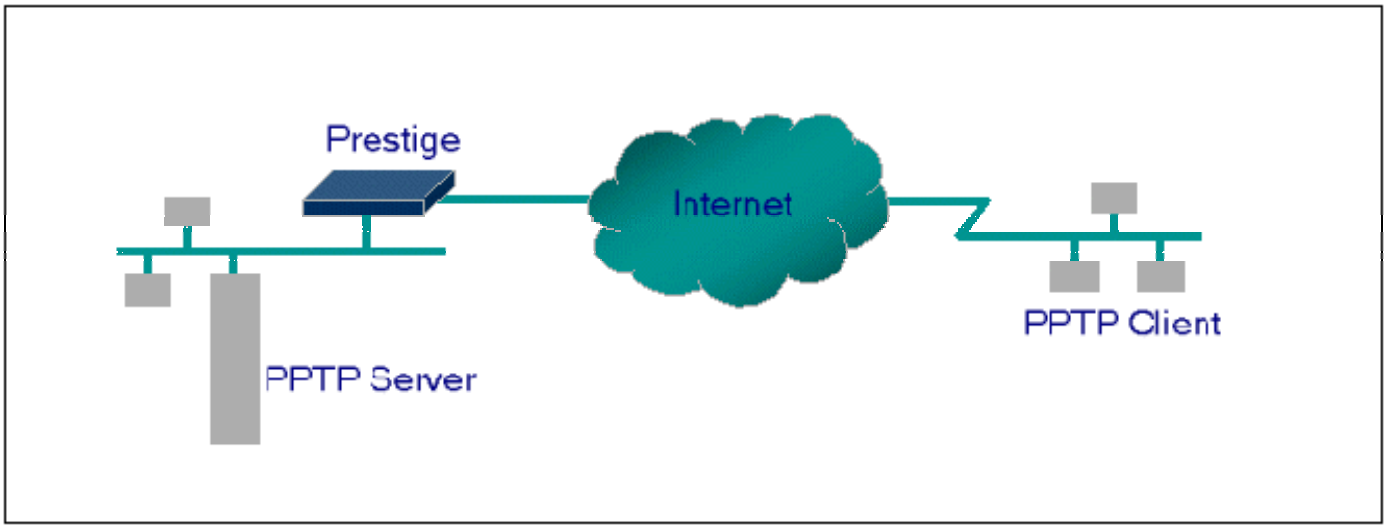
Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

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, 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 already supported in Windows NT and Windows 98. For Windows 95, a software upgrade with Dial-Up Networking 1.2 is required.

- Configuration

This application note explains how to establish a PPTP connection to a remote private network on the Prestige with SUA enabled. In ZyNOS, all PPTP packets are forwarded to the internal PPTP Server (Windows NT server) behind SUA. . You must specify the PPTP port number in SMT menu 15 for the Prestige to forward the packets to the intended Windows NT server using the private IP address.



- Example

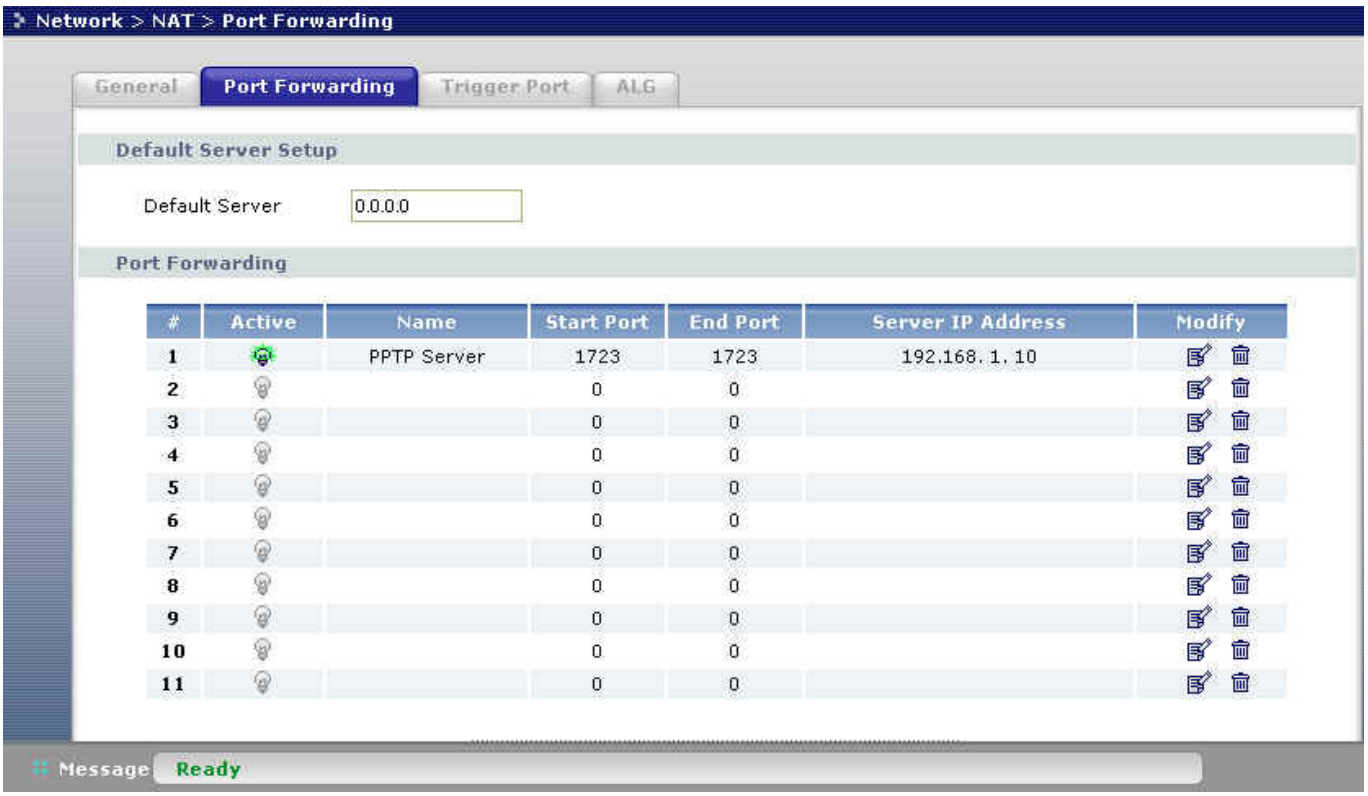
The following example shows how to dial to an ISP via the Prestige and then establish a tunnel to a private network. You need to configure the settings on a PPTP server (such as a Windows NT server), a PPTP client (Windows 9x) and the Prestige to set up the PPTP application. The following summarizes the setting for the corresponding PPTP device.

- PPTP server setup (Windows NT)
  - Create a new VPN service in Control Panel>Network
  - Create a new PPTP user account
  - Enable the RAS port
  - Select a network protocol (such as IPX, TCP/IP or NetBEUI) for the RSA port
  - Set the Prestige as the Internet gateway
- PPTP client setup (Windows n9x)

- In Dial-up Networking, create a secure VPN connection through the Prestige (using the WAN IP address) and enter the correct user name and password to log into the Windows NT RAS server.
- Set the Prestige that connects to the ISP as the Internet gateway.

o Prestige Setup

- Before establishing a VPN connection from the PPTP client (Windows 9x) to the PPTP server (Windows NT server), you must first connect the Prestige to the ISP for Internet access.
- Enter the IP address and the port number(s) of the PPTP server to allow public access to the server behind the Prestige. The following shows a configuration example.

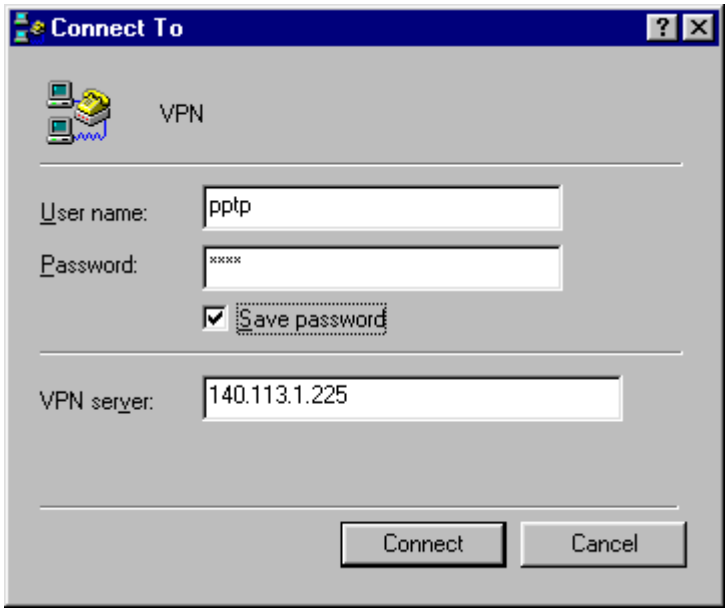


After you have set the settings to allow public access to the PPTP server, test the connection from the PPTP client to the PPTP server. You can use Ping to check that the PPTP client can reach the PPTP server over the Internet connection. For example, enter "ping 203.66.113.2" if the WAN IP address of the Prestige is 203.66.113.2.

Once the connection is up, you can establish a secure VPN connection from the PPTP client to the ISP. The default gateway is then used to route the traffic between the PPTP client and the server.

However, before you can establish a secure VPN connection from the PPTP client to the PPTP server, you need to know the WAN IP address of the Prestige with the SUA feature enabled. Depending on your Internet account type and ISP, the Prestige WAN IP address is either fixed(static) or dynamic (different each time). You need to enter the WAN IP address of the Prestige in the VPN dial-up connection screen. You can check the WAN IP address of the Prestige in SMT menu 24.1 or using PNC Monitor. If the Prestige is using a fixed (static) IP address, you can always use this fixed IP address to connect to the PPTP server.

The following figure shows an example VPN dial-up screen. The VPN Server field is 140.113.1.225 which is a dynamic IP address assigned to the Prestige by the ISP. Make sure you enter the WAN IP address of the Prestige correctly; otherwise, the VPN connection will fail. After the VPN connection is established, you can start using Internet applications (such as on-line games).



About Filters & Filter Examples

How does the ZyXEL filter feature work?

- **Filter Structure**

The Prestige allows you to configure up to twelve filter sets with six rules in each set (for a total of 72 filter rules on the Prestige). You can apply up to four filter sets on a port to block packets that match the rules. Since you can configure up to six filter rules in a set, you can apply up to 24 filter rules on a port. The following figure shows the logic flow of a filter rule on the Prestige.

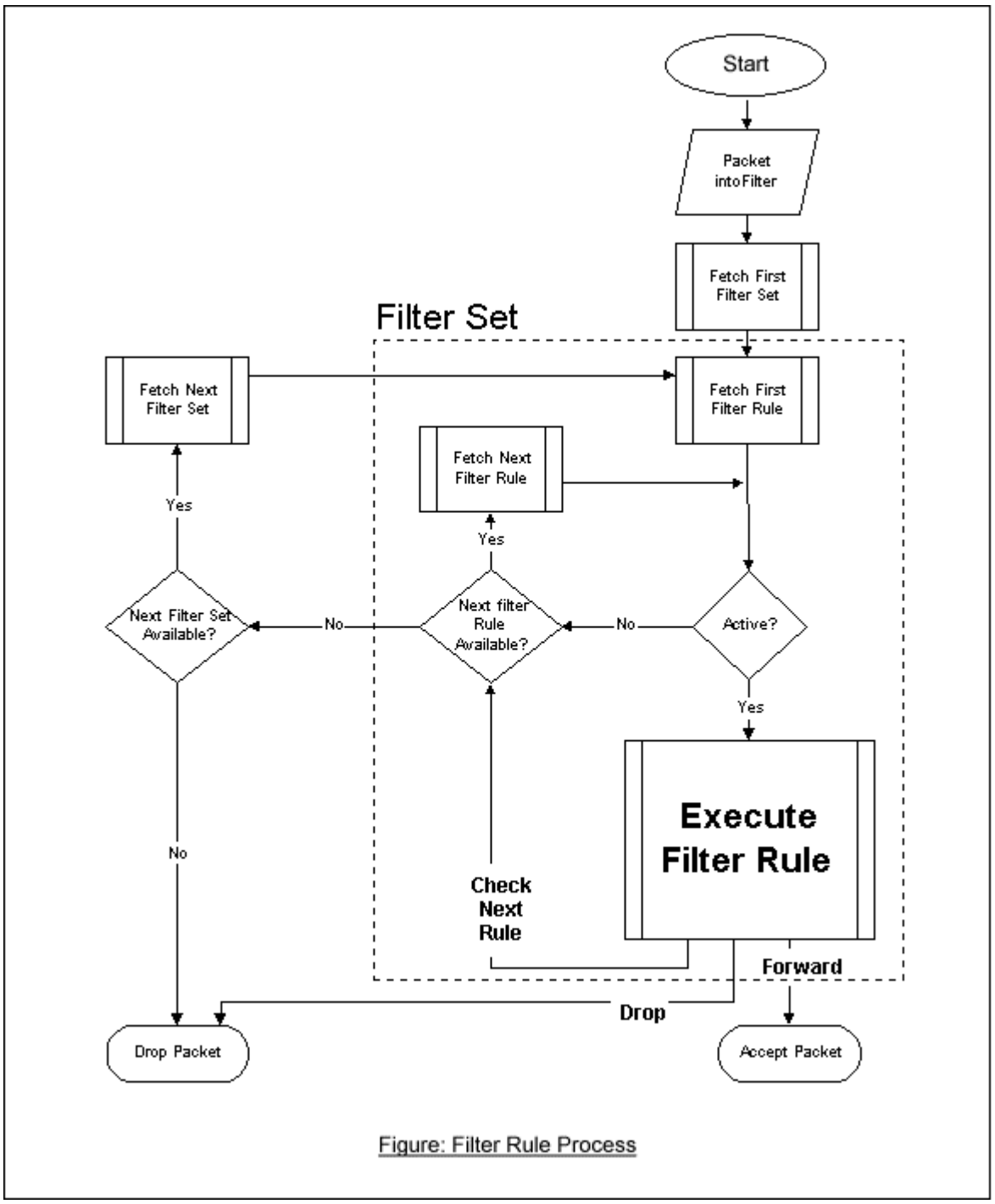


Figure: Filter Rule Process

- **Filter Types and SUA**

You can configure two filter rule categories: 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.

TCP/IP filters are applied before SUA address translation on outgoing traffic to the WAN and after SUA address translation on incoming traffic from the WAN. This allows the Prestige to apply the filters with the specified IP address and port number accurately before SUA.

Generic filters are applied at the point of transmission. For example when the traffic is received or transmitted on an interface.

Figure1 shows the filter logic flow sequence. Steps of the logic flow sequence for LAN-to-WAN traffic are listed below.

- LAN device and protocol input filter sets.
- WAN protocol call and output filter sets.
- If SUA is enabled, SUA changes 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.

Steps of the logic flow sequence for WAN-to-LAN traffic are listed below.

- WAN device input filter sets.
- If SUA is enabled, SUA changes 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.

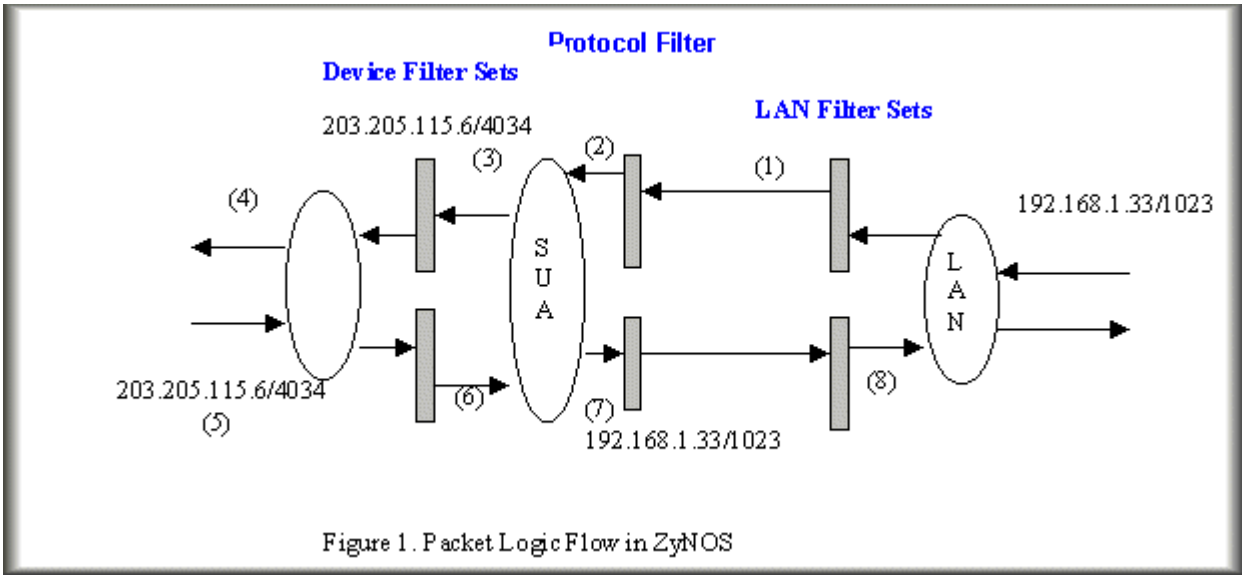


Figure 1. Packet Logic Flow in ZyNOS

Generic and TCP/IP (and IPX) filter rules are in different filter sets. You can only activate one type of filter rules on the Prestige. The SMT automatically detects and prevents you from activating two filter types at the same time. If you configure a Generic and a TCP/IP filter rule (as shown in the following figures) and try to activate them at the same time, the 'Protocol and device filter rules cannot be active together' error message displays.

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
```

You have to apply the protocol and device filters separately (in SMT menu 3.1 and 11.5). This prevents you from mistakenly applying the wrong filters. The menus are modified to include new fields as 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=
```

The SMT does not allow you to apply a protocol filter set (configured in menu 21) to the **device filters** field in menu 3.1 or 11.5. Likewise, you cannot apply a device filter in the **protocols filters** field. However, the SMT cannot detect whether you have configured device and protocol filter rules in the same filter set. This was

allowed in the pre-ZyNOS v3.40 firmware. Thus when you upgrade the firmware to ZyNOS v3.40, the old configuration is translated to the new format and any filter configuration inconsistence is logged. It is highly recommended that you check the system log (in SMT menu 24.3.1) before setting up the device on the network.

Note: The Prestige automatically deactivates the routing/bridging functions when an inconsistency is detected in the filter rule settings.

Filter to block web services

- Configuration

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

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

Generally, the outbound packets for a web service could be as follows:

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

To block web services on all LAN hosts, enter 0.0.0.0 for the source IP address. Otherwise enter the IP address of a LAN computer to block web services for that computer. The configuration procedure is described below.

- Create a filter set in SMT menu 21, for example, set 1
- Create three filter rules in menu 21.1.1, 21.1.2, and 21.1.3
  - Rule 1- block the HTTP packets, TCP (06) protocol type with port number 80
  - Rule 2- block the DNS packets, TCP (06) protocol type with port number 53
  - Rule 3- block the DNS packets, UDP (17) protocol type with port number 53
- 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. Configure rule one for (a). HTTP packets using TCP(06) and 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. Configure rule 2 for (b). DNS requests using TCP(06) and 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 packets using UDP(17) and port number 53.

```
                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 #= 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 configured, 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 in the **'Output Protocol Filter Set'** field for the remote node.

A filter to block a specific client

Configuration

1. Create a filter set in SMT menu 21, for example, 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.Create one rule to block 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 IP address of the computer you want to block in this field
IP Mask.....Enter the IP subnet mask bits in this field. For example, to block only one computer, enter 255.255.255.255.
Action Matched.....Select 'Drop' to discard all the packets from this computer
Action Not Matched.....Select 'Forward' to allow the packets from other computers.

3. After you have configure the filter rule, you can apply this filter set in the (by entering "1") in the 'Output Protocol Filter Set' field for remote node setup.

A filter to block a specific MAC address

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

Before you Begin

Before you configure the filter, you need to know the MAC address of the computer first. Check the MAC address of the network card on the computer (for example, you can use the "ipconfig -all" command or check the system hardware information). Also, you can use packet trace on the Prestige to identify packets with the specified MAC address. The following figure shows a packet trace example.

```
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 following shows detailed information with 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 packet trace example above, we know that a client is trying to ping the Prestige. And from the second trace using Ethernet Version II, we know the Prestige will send a reply to the client. The following sample generic filter is configured to block the MAC address [00 80 c8 4c ea 63].

1. First, from the incoming packet on the LAN, the source MAC address to block 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. Based on the information obtained, configure the generic filter rule as shown 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 Rule
  Select **Generic Filter Rule** in the **Filter Type** field.

- Active
  Select **Yes** in the **Active** field.

- Offset (in bytes)
  Enter 6 for the offset since the source MAC address starts at the 7th octet. This will set the Prestige to bypass checking on the first 6 octets (the destination MAC address).

- Length (in bytes)
  Enter 6 for the length since a MAC address has 6 octets.

- Mask (in hexadecimal)
  Specify the value that the Prestige will logically qualify (logical AND) the data in the packet.
  Since the Length is set to 6 the Mask should be 12 hexadecimal numbers. In this case, enter '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 Prestige should use to compare with the masked packet. If the result from the masked packet matches the 'Value' field, then the packet is considered a match.

- Action Matched=
  Enter the action on the matched packets. In this case, we will drop it.

- Action Not Matched=
  Enter the action on packets that do not match the mask. In this example, we will forward it. If you want to configure more rules, select 'Check Next Rule' to start configuring a next rule. However, note that the new rule 'Filter Type' must be of the same type (in this example, 'Generic Filter Rule'). You must configure the Generic and TCPIP (IPX) filter rules 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 the generic filter rule set in SMT Menu 3.1 - General Ethernet Setup. Note that you can only select 'Generic Filter' in the 'Device Filter' field, but not in the 'Protocol Filter' field which allows you to apply 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 to block NetBIOS packets

- Introduction

The NETBIOS protocol allows the sharing of Microsoft computers in a workgroup. For security reasons, the Prestige blocks NetBIOS connections from the outside by default. To enable the NetBIOS service, remove the filter sets applied in SMT menus 3.1 and 4.1. The details of the filter settings are described as follows.

- Configuration

The following lists the packets that are blocked. Configure the rules in the filter set 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 you can configure the filter rules, enter a descriptive name for the filter set in the **Comments** field.

```
                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 for the 'NetBIOS_WAN' filter set by entering 1 in the **Enter Filter Set Number to Configure** field.

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

```
                    Menu 21.1.1 - TCP/IP Filter Rule
```

```
                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 6      IP Source Route= No
                Destination: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 137
                             Port # Comp= Equal
                     Source: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 0
                             Port # Comp= None
                TCP Estab= No
                More= No            Log= None
                Action Matched= Drop
                    Action Not Matched= Check Next Rule
                Press ENTER to Confirm or ESC to Cancel:
```

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

```
                     Menu 21.1.2 - TCP/IP Filter Rule
                Filter #: 1,2
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 17     IP Source Route= No
                Destination: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 137
                             Port # Comp= Equal
                     Source: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 0
```

```
                Port # Comp= None
        TCP Estab= N/A
        More= No            Log= None
        Action Matched= Drop
        Action Not Matched= Check Next Rule
        Press ENTER to Confirm or ESC to Cancel:
```

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

```
             Menu 21.1.3 - TCP/IP Filter Rule
        Filter #: 1,3
        Filter Type= TCP/IP Filter Rule
        Active= Yes
        IP Protocol= 6      IP Source Route= No
        Destination: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #= 138
                     Port # Comp= Equal
             Source: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #= 0
                     Port # Comp= None
        TCP Estab= No
        More= No            Log= None
        Action Matched= Drop
        Action Not Matched= Check Next Rule

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

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

```
     Menu 21.1.4 - TCP/IP Filter Rule
Filter #: 1,4
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17    IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 138
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 0
             Port # Comp= None
TCP Estab= N/A
More= No           Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

```
     Menu 21.1.5 - TCP/IP Filter Rule
Filter #: 1,5
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6     IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 139
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
```

```
                Port #= 0
                Port # Comp= None
        TCP Estab= No
        More= No            Log= None
        Action Matched= Drop
        Action Not Matched= Check Next Rule
        Press ENTER to Confirm or ESC to Cancel:
```

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

```
             Menu 21.1.6 - TCP/IP Filter Rule
        Filter #: 1,6
        Filter Type= TCP/IP Filter Rule
        Active= Yes
        IP Protocol= 17     IP Source Route= No
        Destination: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #= 139
                     Port # Comp= Equal
             Source: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #= 0
                     Port # Comp= None
        TCP Estab= N/A
        More= No            Log= None
        Action Matched= Drop
        Action Not Matched= Forward

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

- After you have configured the rules for the first filter set, view the filter rule summary in SMT menu 21.2.

```
          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' in the **'Output Protocol Filter'** field for the remote node setup.

Configure the second filter set 'NetBIOS_LAN' by entering 2 in the Filter Set field.

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

```
                    Menu 21.2.1 - TCP/IP Filter Rule
                Filter #: 2,1
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 6     IP Source Route= No
                Destination: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 53
                             Port # Comp= Equal
                     Source: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 137
                             Port # Comp= Equal
```

```
TCP Estab= No
More= No            Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

```
     Menu 21.2.2 - TCP/IP Filter Rule
Filter #: 2,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17    IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 53
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 137
             Port # Comp= Equal
TCP Estab= N/A
More= No            Log= None
Action Matched= Drop
Action Not Matched= Forward
Press ENTER to Confirm or ESC to Cancel:
```

1. After you have configured the second filter set, view the filter rule settings in SMT menu 21.2.

```
           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
```

1. Apply the 'NetBIOS_LAN' filter set in the **'Input protocol filters='** field in SMT menu 3.1 to block packets from the LAN.

```
            Menu 3.1 - General Ethernet Setup

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

Using Dynamic DNS (DDNS)

1. What is DDNS?

A DNS (Domain Name Service) server stores the mappings of IP address and domain names. For example, when users enters a web site address (the domain name), the DNS server automatically maps the web site address to a public IP address and redirects the request to the intended web server.

Without DNS, users have to enter the IP address of the web server in order to access the web sites. This is very inconvenient and not user-friendly as users have to remember the IP addresses of the web sites.

However, if the web server is located behind the Prestige which is using a dynamic WAN IP address, a fixed mapping cannot be stored in the DNS server database since the WAN IP address changes. Thus Dynamic DNS (DDNS) is used to solve this problem. For example, if you have hosted a web site (say www.zyxel.com) on a server behind the Prestige which is assigned a dynamic WAN IP address from the ISP, users can still access the

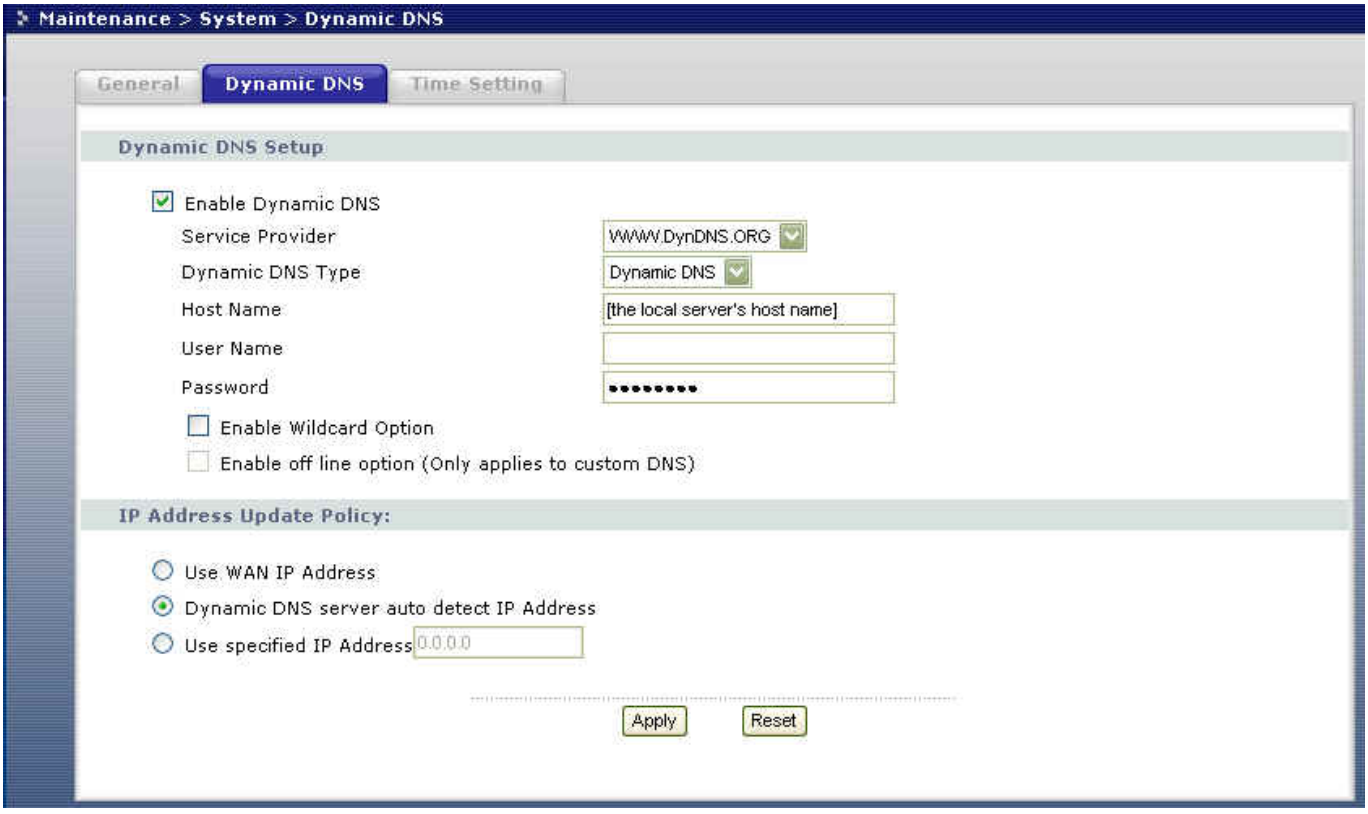
web site from the WAN when you have set up the DDNS settings. With DDNS, users can always access a web site regardless of the WAN IP address on the Prestige.

When the ISP assigns the Prestige a new WAN IP address, the Prestige sends this information to the DDNS server which updates the IP-to-DNS mapping. Once the mapping is updated, outside users can still access the web site hosted on an internal server behind the Prestige.

You must register an account with a DDNS service provider. The DDNS server saves the password-protected e-mail address with the IP addresses and host names. Queries are serviced based on the e-mail addresses. Thus you must set the same e-mail address you used for DDNS in the Prestige SMT menu 1.

Currently, the Prestige supports WWW.DYNDNS.ORG for the DDNS service. The following describes the setup procedure.

- Register an access with WWW.DYNDNS.ORG DDNS service provider. You will be provided with a hostname for the internal server and a password for the IP address update on the DDNS server.
- Configure the DDNS settings on the Prestige. Log into the WEB GUI on the Prestige and click **Maintenance > System > Dynamic DNS** to display the configuration screen as shown.



Field Settings for DDNS:

Option	Description
Service Provider	Enter the DDNS server in this field. Currently the Prestige supports WWW.DYNDNS.ORG.
Host	Enter the hostname given by the DDNS service provider. For example, zyxel.com.tw.
User	Enter the user name that the DDNS service provider gives to your.
Password	Enter the password that the DDNS service provider gives to you.
Enable Wildcard	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that the Wildcard option is available from the WWW.DYNDNS.ORG DDNS service provider.

Network Management Using SNMP

1. SNMP Overview

Simple Network Management Protocol (SNMP) is an applications-layer protocol used to exchange management information between network devices (such as routers and switches). By using SNMP, network administrators can easily monitor network devices, detect and solve network problems. SNMP is a member of the TCP/IP protocol suite and 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 enhance SNMP's security capabilities. SNMP encompasses three main areas:

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

Operations allowed are: Get, GetNext, Set, and Trap. These functions operate based on variables stored on network nodes. Examples of variables include statistic counters and node port status. All SNMP management functions are carried out through these simple operations. No action operations are available, but these can be simulated by the setting the variable flags. For example, to reset a node, a counter variable called 'time to reset' can be set to a value which causes 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 set of variables that each node supports is called the *Management Information Base* (MIB). 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 types (including TCP, IP, UDP, SNMP, etc.) 'system' and 'interface.'

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

6. Reads

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

7. Writes

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

8. Traversal operations

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

9. Traps

The managed devices asynchronously report certain events to NMSs using traps.

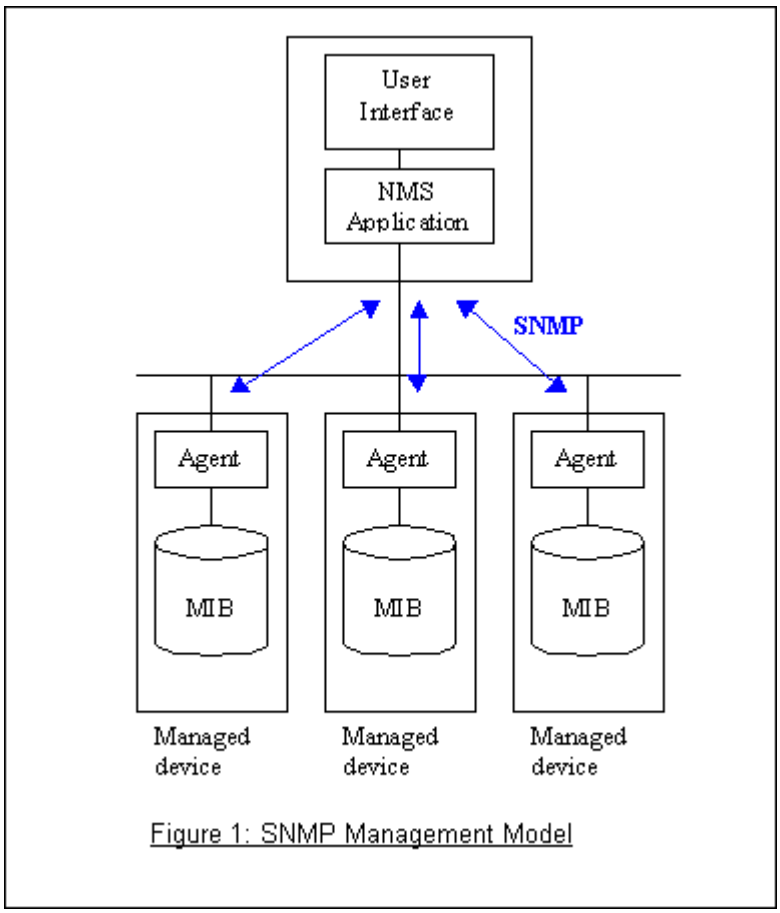


Figure 1: SNMP Management Model

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

There are two parts in an SNMPv1 message. The first part contains a version number and a community name. The second part contains the actual SNMP protocol data unit (PDU) specifying the operation to be performed

(Get, Set, etc.) and the object values involved in the operation. The following figure shows the SNMPv1 message format.

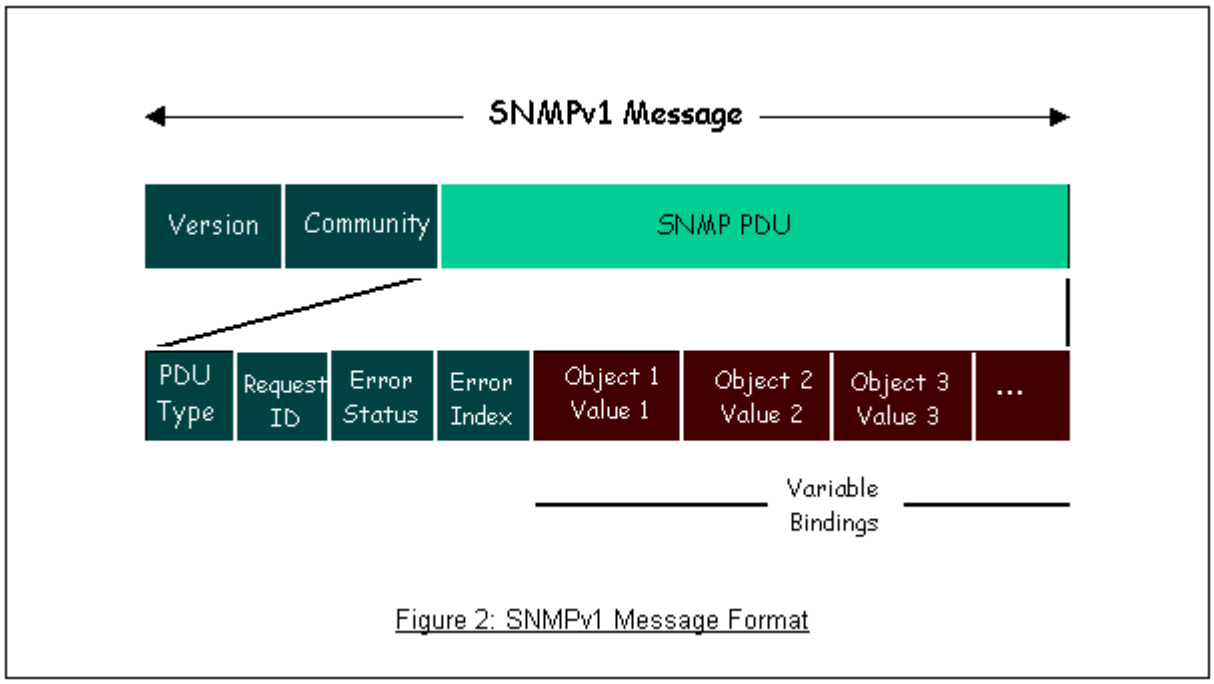


Figure 2: SNMPv1 Message Format

An 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 an object variable.
- **Variable-bindings** Associates an object with its value.

3. ZyXEL SNMP Implementation

Currently, some Prestige models support SNMPv1 that allows the Prestige to communicate with SNMPv1 NMSs. For SNMPv1 operation, ZyXEL allows one community string so that the Prestige can only belong to one community and allows trap messages to be sent to only one NMS manager.

The following describes some common traps and the corresponding events.

- coldStart (defined in RFC-1215) :

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

- warmStart (defined in RFC-1215) :

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

- linkDown (defined in RFC-1215) :

  If a DSL or WAN link is down, the trap will be sent with the port number . The port number is its interface index in the interface group.

- linkUp (defined in RFC-1215) :

  If a DSL or WAN link up, the trap will be sent with the port number . The port number is its interface index in the interface group.

- authenticationFailure (defined in RFC-1215) :

When the wrong community (password) is received for an SNMP get or set operation, , this trap is sent to the manager.

1. 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 (such as downloading new files or entering the "sys reboot" command, ...), a system reboot is done intentionally. And traps with the message "System reboot by user !" will be sent.

(ii) For fatal error :

In case the system has to reboot due to unrecoverable errors. Traps with the error codes will be sent.

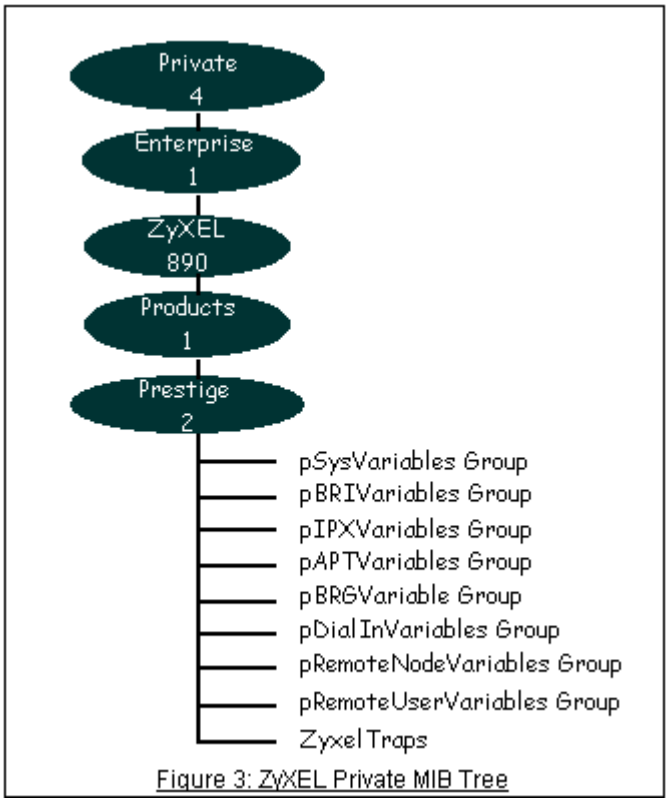
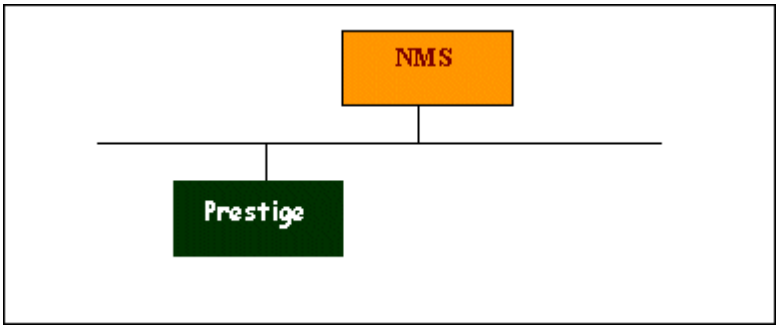
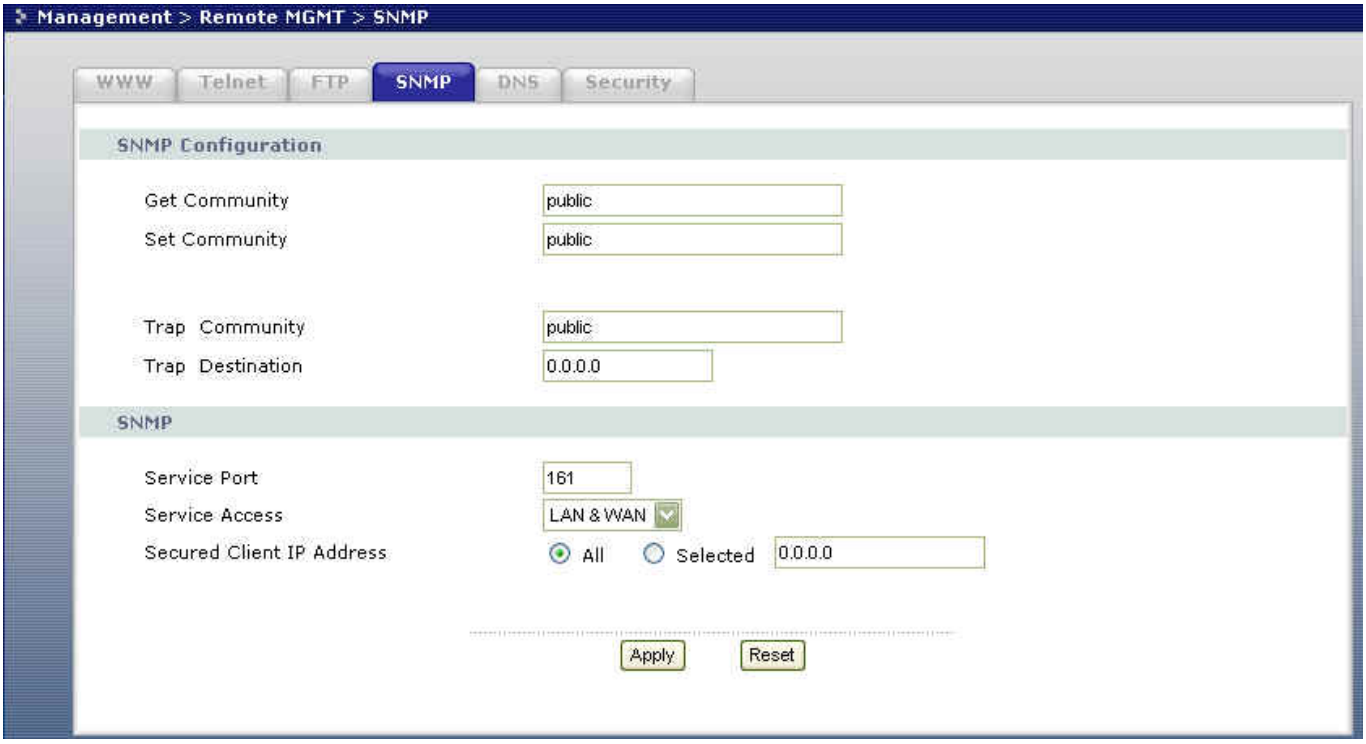


Figure 3: ZyXEL Private MIB Tree

4. Configure the Prestige for SNMP



You can configure SNMP related settings on the Prestige in the WEB GUI. Log into the WEB GUI, click Management > Remote MGMT > SNMP.



Field Settings for SNMP:

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 Prestige will only respond to the SNMP messages from this IP address. **If you enter 0.0.0.0 , the Prestige 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 Prestige will not send traps to any NMS manager.**

Using syslog

4. **Prestige Setup**

Configuration:

1. Active: Select this check box to enable syslog logging.
2. Syslog IP Address: Enter the IP address of the syslog server that you wish to send the syslog.
3. Log Facility: Select a log location (numbered 1 to 7).

- **UNIX Setup**

1. Make sure that you start syslogd with the *-r* argument.

-r allows the syslog facility to receive messages from the network using an Internet domain socket with the syslog services. The default setting is NOT enabled.

2.Add the following commands 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.

- **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 is the Remote Call ID)
C01 Incoming Call xxxx (the connected speed) xxxxx (the Remote Call ID)
L02 Tunnel Connected(L2TP)
C02 OutCall Connected xxxx (the connected speed) xxxxx (the 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
```

- **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 send48 hexadecimal characters to the server

Example:

```
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
```

- **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 filter rules log contents.

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
```

- **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:

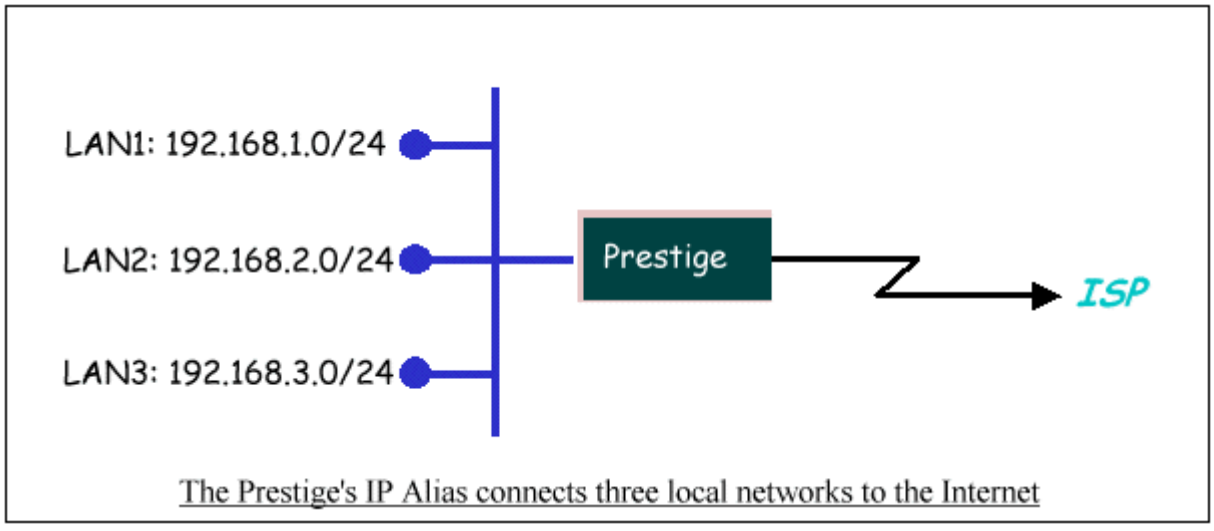
```
Jul 19 11:43:25 192.168.1.1 ZyXEL Communications Corp.: ppp:LCP Starting
Jul 19 11:43:29 192.168.1.1 ZyXEL Communications Corp.: ppp:IPCP Starting
Jul 19 11:43:34 192.168.1.1 ZyXEL Communications Corp.: ppp:CCP Starting
Jul 19 11:43:38 192.168.1.1 ZyXEL Communications Corp.: ppp:BACP Starting
Jul 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
```

Using IP Alias

- What is IP Alias ?

In a typical network environment, a LAN router is required to connect two local networks. The Prestige can connect up to three local networks to the ISP or a remote node. This function is known as 'IP Alias'. You do not need to install another internal router if IP alias is enabled. The following figure shows a typical network example where the Prestige is used. In this example, the LAN network is divided into three sub networks which connect to the Internet through the Prestige. All computers on the LAN networks use the Single User Account on the Prestige to access the Internet.



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

The Prestige supports up to three virtual LAN interfaces on its single physical Ethernet interface. You can configure the first logical network in SMT menu 3.2. Configure the second and third networks (IP Alias 1 and IP Alias 2) in SMT Menu 3.2.1 – IP Alias Setup.

The three internal virtual networks are enif0 for the first logical network, enif0:0 for IP alias 1 and enif0:01 for IP alias 2. Three internal virtual LAN interfaces allow the Prestige to route the packets between the three networks correctly. When you have configured the three logical networks, the Prestige automatically creates

three internal routes to route packets among the three networks correctly. When you enable DHCP server on the Prestige, you can configure the client address pool for any of the networks.

```
Copyright (c) 1994 - 2004 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>
```

To allow or block LAN packets to/from IP alias 1 or 2, apply protocol filters in menu 3.2.1. The filter set(s) applied in SMT menu 3.1 is for the main logical network (configured in menu 3.2).

- IP Alias Setup

1. Configure the first logical network in menu 3.2 by setting the Prestige's LAN IP address.

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


DHCP= Server                        TCP/IP Setup:
Client IP Pool:
  Starting Address= 192.168.1.33    IP Address= 192.168.1.1
  Size of Client IP Pool= 32        IP Subnet Mask= 255.255.255.0
First DNS Server= From ISP          RIP Direction= Both
  IP Address= N/A                     Version= RIP-1
Second DNS Server= From ISP         Multicast= None
  IP Address= N/A                   Edit IP Alias= Yes
Third DNS Server= From ISP
  IP Address= N/A
DHCP Server Address= N/A


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

Field Settings:

DHCP Setup	If the Prestige's DHCP server is enabled, configure the client address pool for any of the three logical networks.
TCP/IP Setup	Enter the first LAN IP address for the Prestige. This will create the first route entry on the enif0 interface.
Edit IP Alias	Press [SPACE] to select **Yes** and press enter to display SMT Menu 3.2.1 – IP Alias Setup to configure the second and third logical networks on the Prestige.

2. In menu 3.2.1, set the LAN IP address for the second and third logical networks on the Prestige.

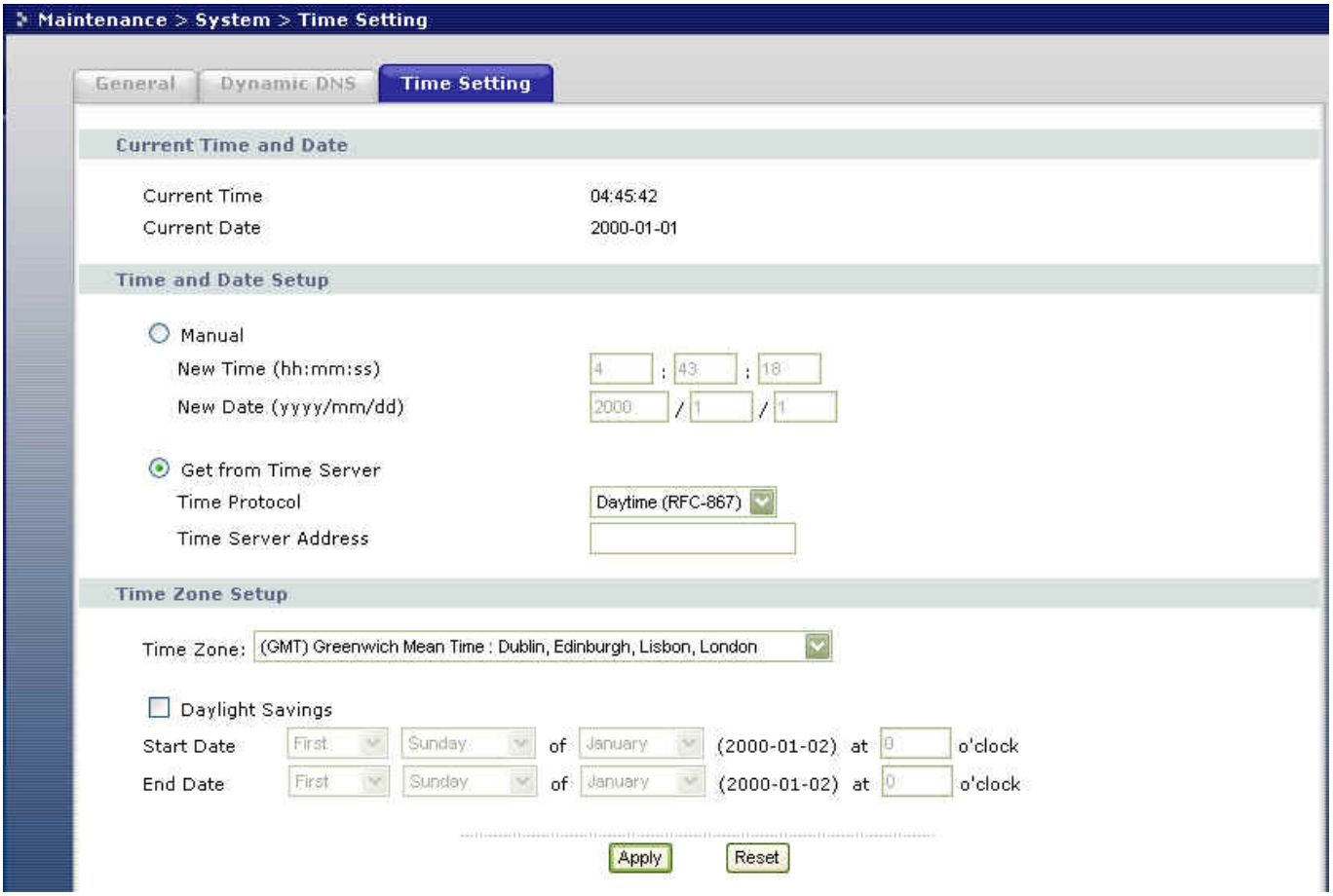
```
                Menu 3.2.1 - IP Alias Setup
          IP Alias 1= Yes
            IP Address= 192.168.2.1
            IP Subnet Mask= 255.255.255.0
            RIP Direction= None
            Version= RIP-1
            Incoming protocol filters=
            Outgoing protocol filters=
          IP 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:
```

Field Settings:

IP Alias 1	Select **Yes** and enter the LAN IP address for the second logical network on the Prestige. This will create the second route entry on the enif0:0 interface.
IP Alias 2	Select **Yes** and enter the LAN IP address for the third logical network on the Prestige. This will create the second route entry on the enif0:1 interface.

- System Date and Time Settings on the Prestige

Since the Prestige does not contain a RTC (Real-Time Clock) chip, you need to set the Prestige to obtain the current time and date information from an external time server during system booting. You can set the Prestige to use Daytime protocol(RFC-867), Time protocol(RFC-868) or NTP protocol(RFC-1305) time service. To use the time service, you need to specify the IP address of the external time server. Once configured, the Prestige is able to obtain the current time, date and the time zone information from the external time server.



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 for multicasting. There are currently two versions: versions 1 and 2. Through IGMP, IP hosts are able to report their multicast group membership to any immediate-neighbor multicast routers which decide if a multicast packet needs to be forwarded.

At start up, the Prestige queries all directly connected networks to gather group membership information. The Prestige then updates the information through periodic queries.

The Prestige supports IGMP versions 1 and 2. You can enable/disable multicast setting on the Ethernet interface or to the remote node.

- IP Multicast Setup

Enable IGMP on the Prestige's LAN interface in menu 3.2:

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

DHCP= Server                          TCP/IP Setup:

Client IP Pool:

  Starting Address= 192.168.1.33      IP Address= 192.168.1.1

  Size of Client IP Pool= 32          IP Subnet Mask= 255.255.255.0

First DNS Server= From ISP            RIP Direction= Both

  IP Address= N/A                       Version= RIP-1

Second DNS Server= From ISP           Multicast= IGMP-v2
```

```
    IP Address= N/A                    Edit IP Alias= No

Third DNS Server= From ISP

    IP Address= N/A

DHCP Server Address= N/A

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

Enable IGMP for a remote node in menu 11.3:

```
              Menu 11.3 - Remote Node Network Layer Options

                IP Address Assignment= Dynamic
                Rem IP Addr= N/A
                Rem Subnet Mask= N/A
                My WAN Addr= N/A

                Network Address Translation= SUA Only
                Metric= 1
                Private= No
                RIP Direction= Both
                  Version= RIP-2B
                Multicast= IGMP-v2

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

Field Settings:

Multicast	Select IGMP-v1 for IGMP version 1 or IGMP-v2 for IGMP version 2.

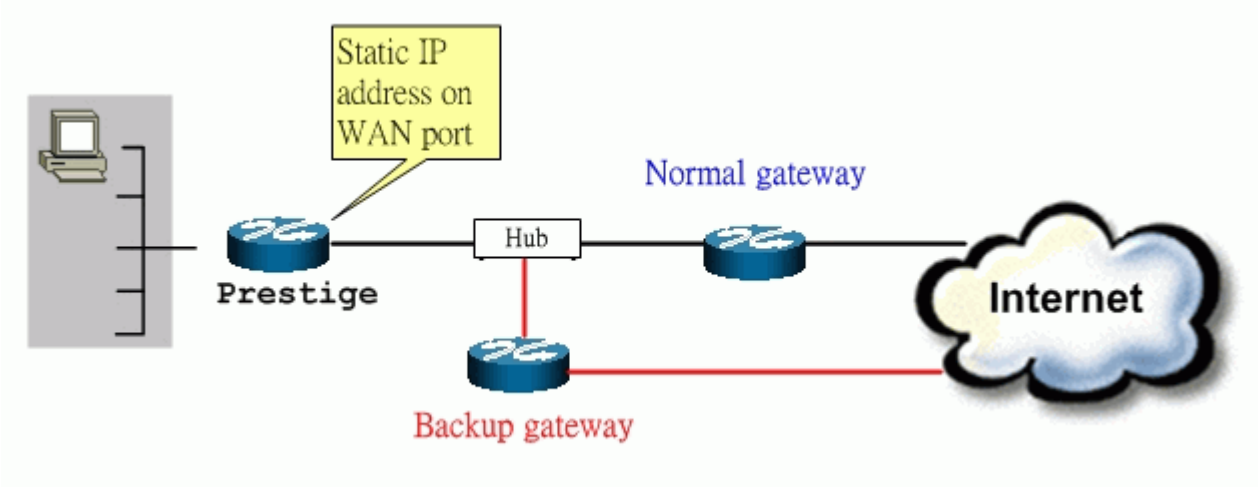
Using Prestige traffic redirect

- What is Traffic Redirect ?

Traffic redirect forwards WAN traffic to a backup gateway when the Prestige cannot connect to the Internet through its normal gateway. Thus this allows your backup gateway to work as an auxiliary backup for the WAN connection. Once the WAN connection is down, the Prestige forwards the outgoing traffic through the backup gateway configured in the traffic redirect settings.

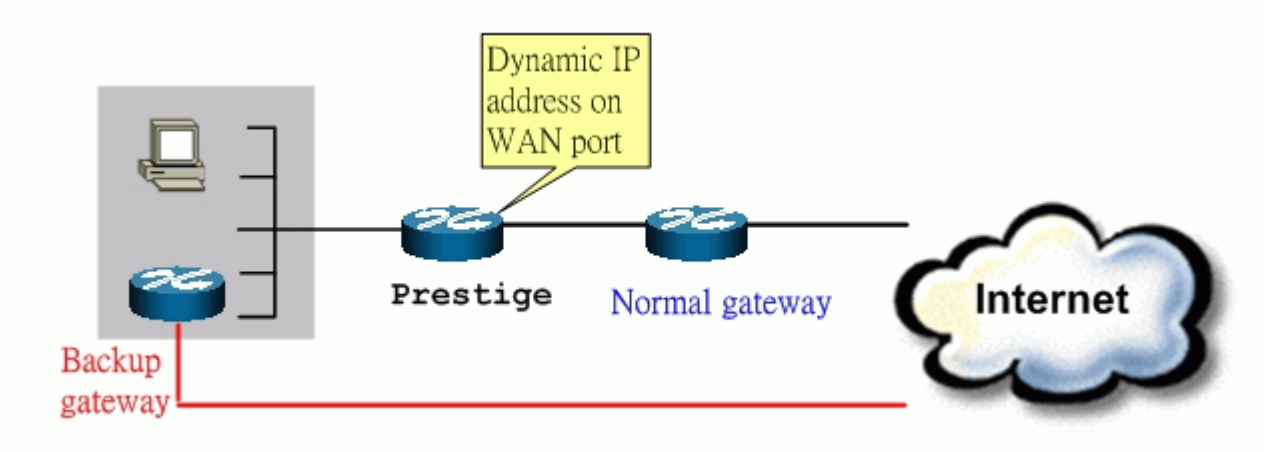
- How to set up the backup gateway?

Set up the backup gateway device on the Prestige' s LAN or WAN. If you want to install the backup gateway on the WAN, make sure the Prestige is using a static (fixed) IP address. The following figure shows an example. If you are not given a static WAN IP address, set the backup gateway on the LAN.



Traffic Redirect on the WAN

If the Prestige is using a dynamic WAN IP address, connect the backup gateway on the LAN. The following figure shows an example.



Traffic Redirect on the LAN

- Traffic Redirect Setup

In **SMT Menu 2 WAN Backup Setup**, specify the conditions that set the Prestige to forward outgoing traffic to a backup gateway when the DSL connection is down.

In **SMT Menu 11.6-Traffic Redirect Setup,** specify the conditions that set the Prestige to forward outgoing traffic to a backup gateway when the DSL connection is down

```
Menu 11.1 - Remote Node Profile
```

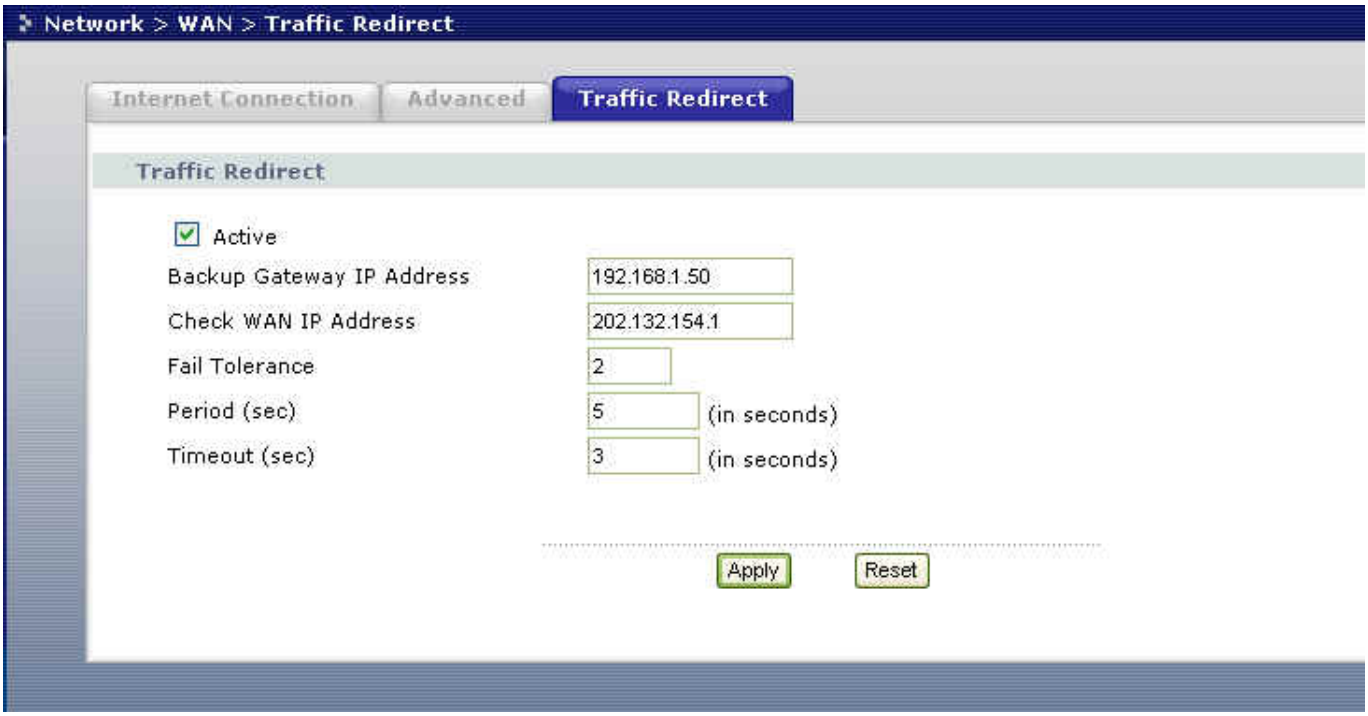
```
                    Menu 11.6 - Traffic Redirect Setup

                Active= Yes
                Configuration:
                  Backup Gateway IP Address= 192.168.1.50
                  Metric= 14
                  Check WAN IP Address= 202.13.154.1
                    Fail Tolerance= 5
                    Period(sec)= 30
                    Timeout(sec)= 3
```

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

Field Settings:

Active	Press [Space BAR] and select **Yes** (to enable) or **No** (to disable) for traffic redirect.
Backup Gateway IP Address	The IP address of your backup gateway. The Prestige automatically forwards outgoing traffic to this IP address if the Prestige's Internet connection is down.
Metric	Enter a number from 1 to 15 to give your traffic redirect route a priority. The smaller the number, the higher priority the route has.
Check WAN IP Address	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable computer nearby (for example, your ISP's DNS server address). The Prestige pings this IP address periodically to check the WAN connection. If you enter 0.0.0.0 in this field, the Prestige checks its default gateway IP address.
Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** fields without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Period	Specify how long the Prestige waits before pinging the IP address to check the WAN connection.
Timeout	Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** fields before timing out the request. The WAN connection is considered "down" after the Prestige times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.

You can also configure traffic redirect in the WEB GUI. Log into the WEB GUI on the Prestige and click ADVANCED > WAN > Traffic Redirect to display the configuration screen.



Using Universal Plug n Play (UPnP)

- **1. What is UPnP**

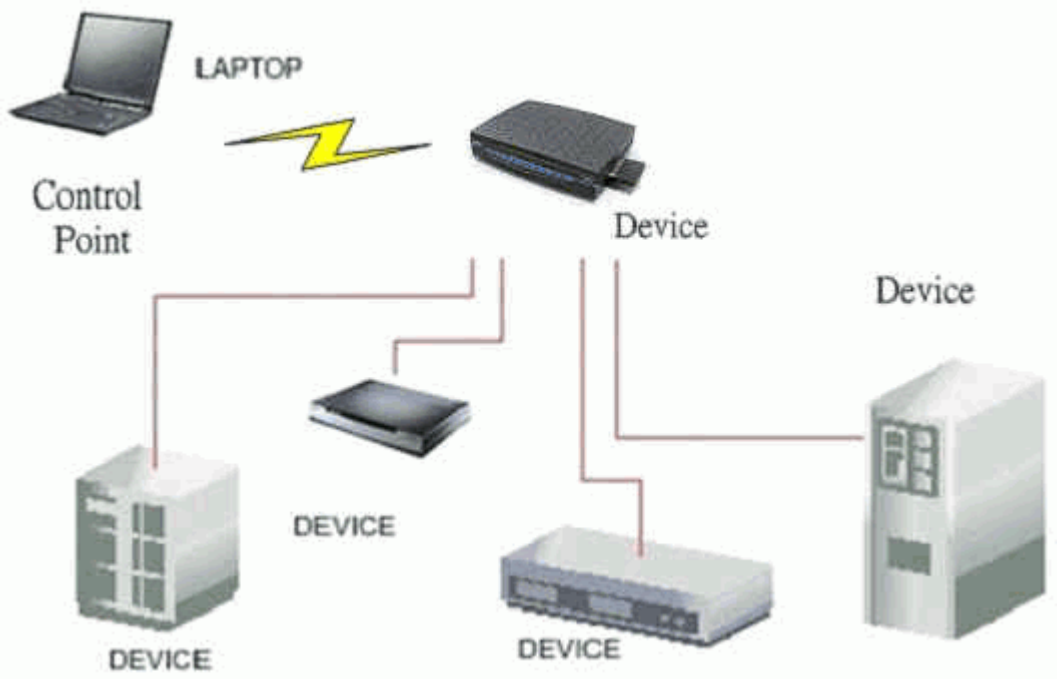
UPnP (Universal Plug and Play) allows you to easily connect to and manage computers, network printers, appliance, wireless devices and other UPnP-capable devices over a home or office network using TCP/IP and web services. UPnP is supported on the latest Windows operating systems and works in both the wired and wireless networks.

UPnP also supports NAT Traversal which solves the connection problem for NAT-unfriendly applications. In UPnP, applications are assigned dynamic port mappings on an Internet gateway. The mappings are temporary as they are deleted when the connection is established.

The following lists and describes the components in a UPnP communication setup.

- **Devices**: Network devices, such as networking gateways, TV, refrigerators, printers...etc, which provides services.

- **Services**: Services are provided by devices, such as time services provided by alarm clocks. In UPnP, services are described in XML format. Control points can set/get services information from devices.
- **Control points**: Control points can manipulate network devices When you add a new control point (in this case, a laptop) to a network, the device may ask the network to find UPnP-enabled devices. These devices then respond with their URLs and device descriptions.



UPnP Operations

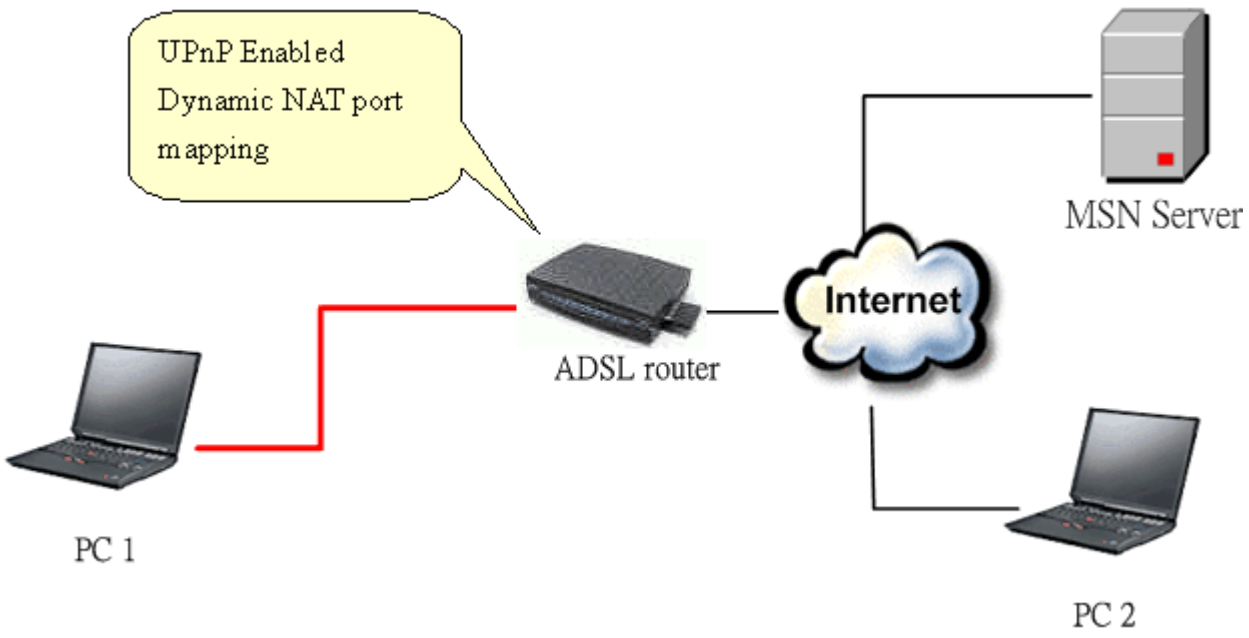
- Addressing: UPnPv1 devices MAY support IPv4, IPv6, or both. For IPv4, each device should be set to work as a DHCP client. When the device is connected to the network, it is able to connect to and obtain IP settings from a DHCP server. If the DHCP server is not found, the device assigns itself an IP address (169.254.0.0/16) using the auto-IP mechanism.
- Discovery: Whenever a device is added to the network, it will advertise its service to other devices on the network. A control point can also discover services provided by the devices.
- Description: Control points can get detailed service information from the devices' description in XML format. The description may include product name, model name, serial number, vendor ID, and embedded services, etc.
- Control: Devices can be manipulated by control points through Control message.
- Eventing: Devices can send event messages to notify control points if there is any update on the services provided.

- Presentation: Each device can provide its own control interface in the form of a URL link. This allows users to access the web management interface on the device by entering the URL address and control the device.

- **2. Using UPnP in ZyXEL devices**

In this example, we will introduce how to enable UPnP in ZyXEL devices. Currently, Microsoft MSN is the most popular application that uses UPnP, so we will use Microsoft MSN as an example. From this example, you will also learn how MSN benefits from the NAT traversal feature in UPnP.

In the following network example, computers PC1 and PC2 are signed in to an MSN server to set up video conferencing. PC1 is connected to a UPnP-enabled router that uses PPPoE Internet connection type. Since the router supports UPnP, no NAP mapping is necessary for PC1. As long as UPnP is activated on the router, a dynamic mapping is automatically created for PC1 on the router. Note that PC1 must also support UPnP (which is available in Microsoft ME or XP).



Device: Prestige
Service: NAT function provided on the Prestige
Control Point: PC1

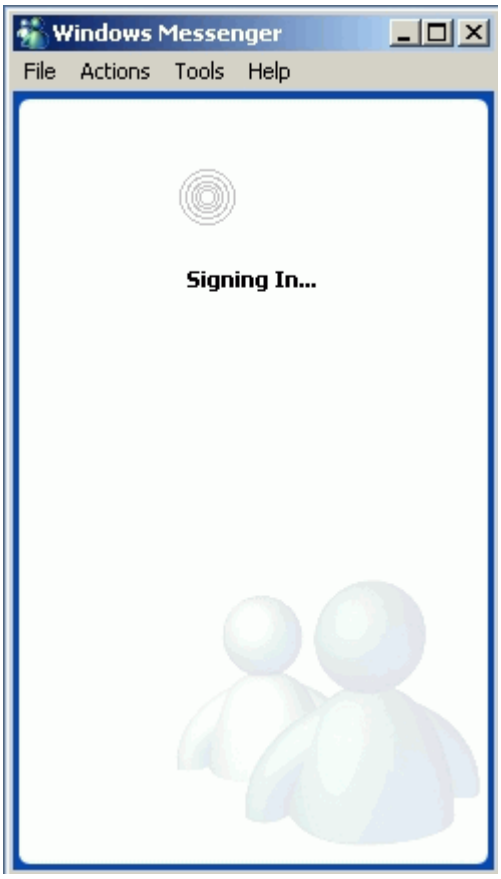
1. Enable the UPnP function in a ZyXEL device

To enable UPnP on a ZyXEL device, log into the web management interface and click Management > UPnP.

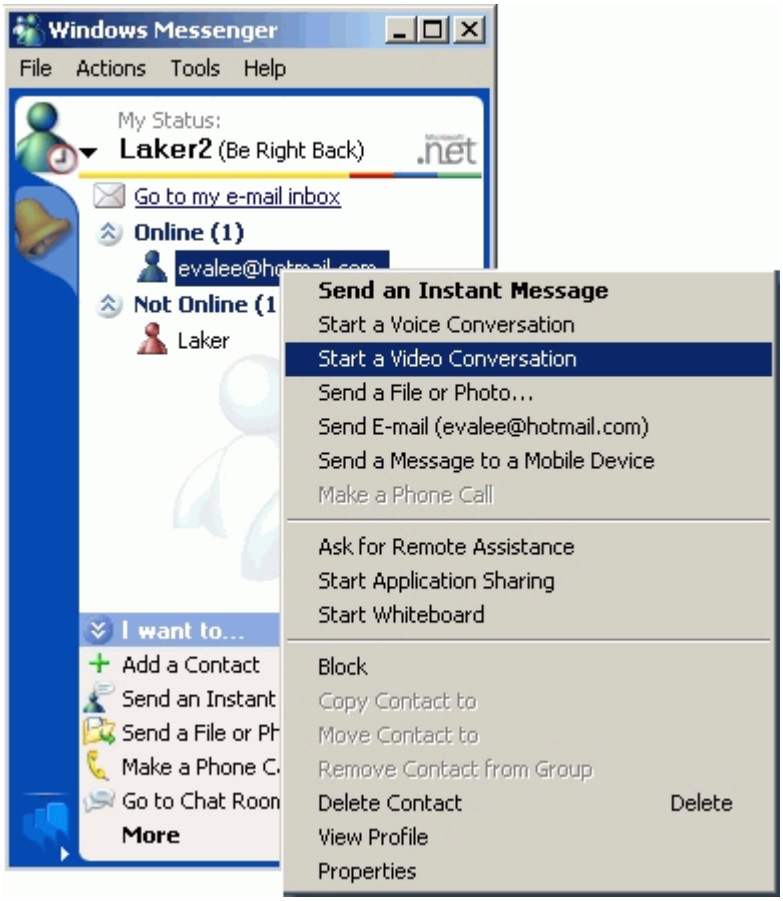
Select **Enable UPnP service** to activate UpnP on the device.

Select the **Allow users to make configuration changes through UPnP** check box allows you to access and change the configuration on the device. For instance, if you select this option, the Prestige automatically creates a dynamic port mapping for your MSN application so your network administrator does not have to set up static SUA port mapping on the Prestige.

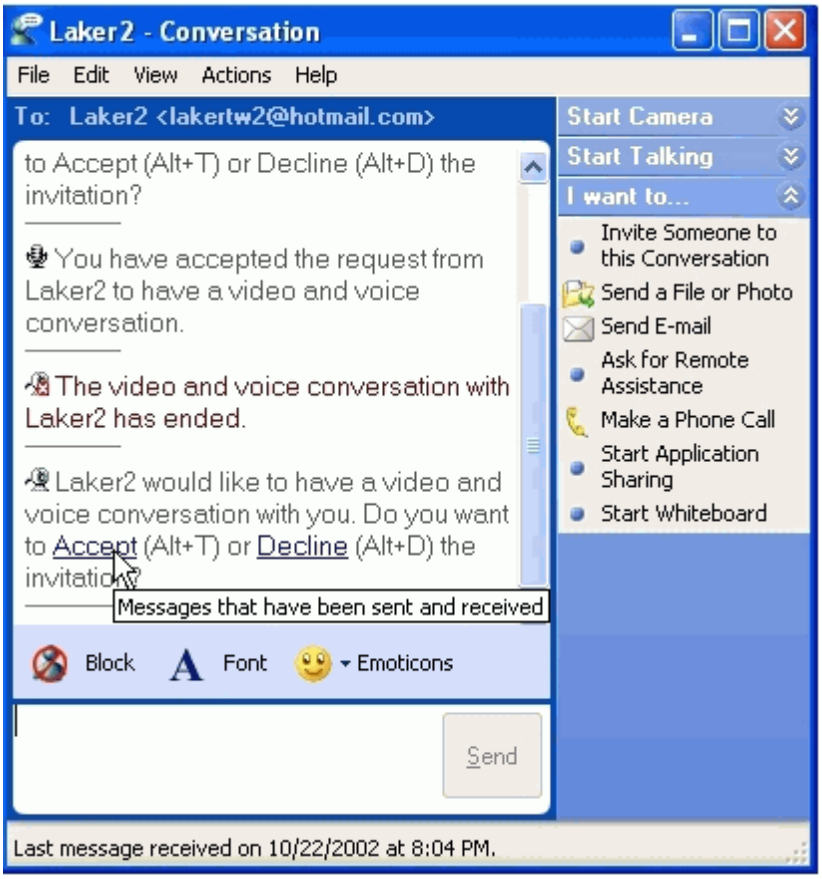
2. After the dynamic port mapping is created and that your computer has obtained an IP address from the Prestige, you can launch the MSN application and connect to the MSN server.



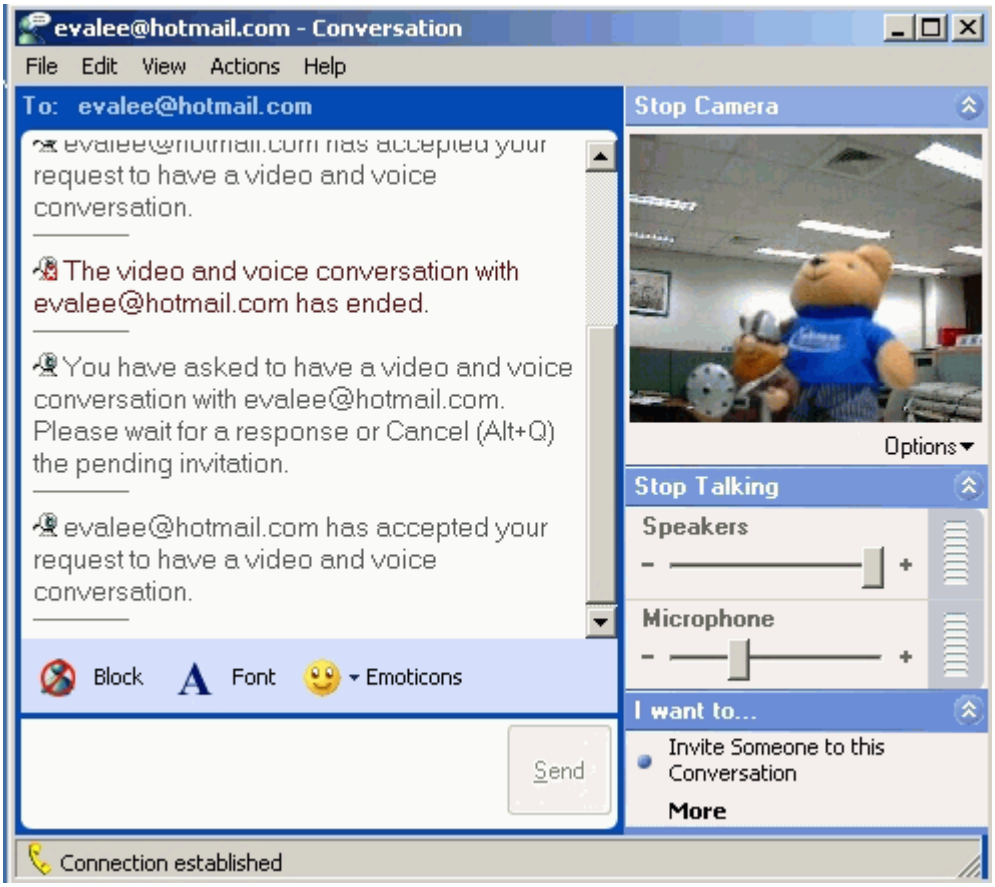
3. After a successful sign-in, you can start a video conversation with another MSN user.



4. The remote MSN user can select Accept to allow your conversation request.



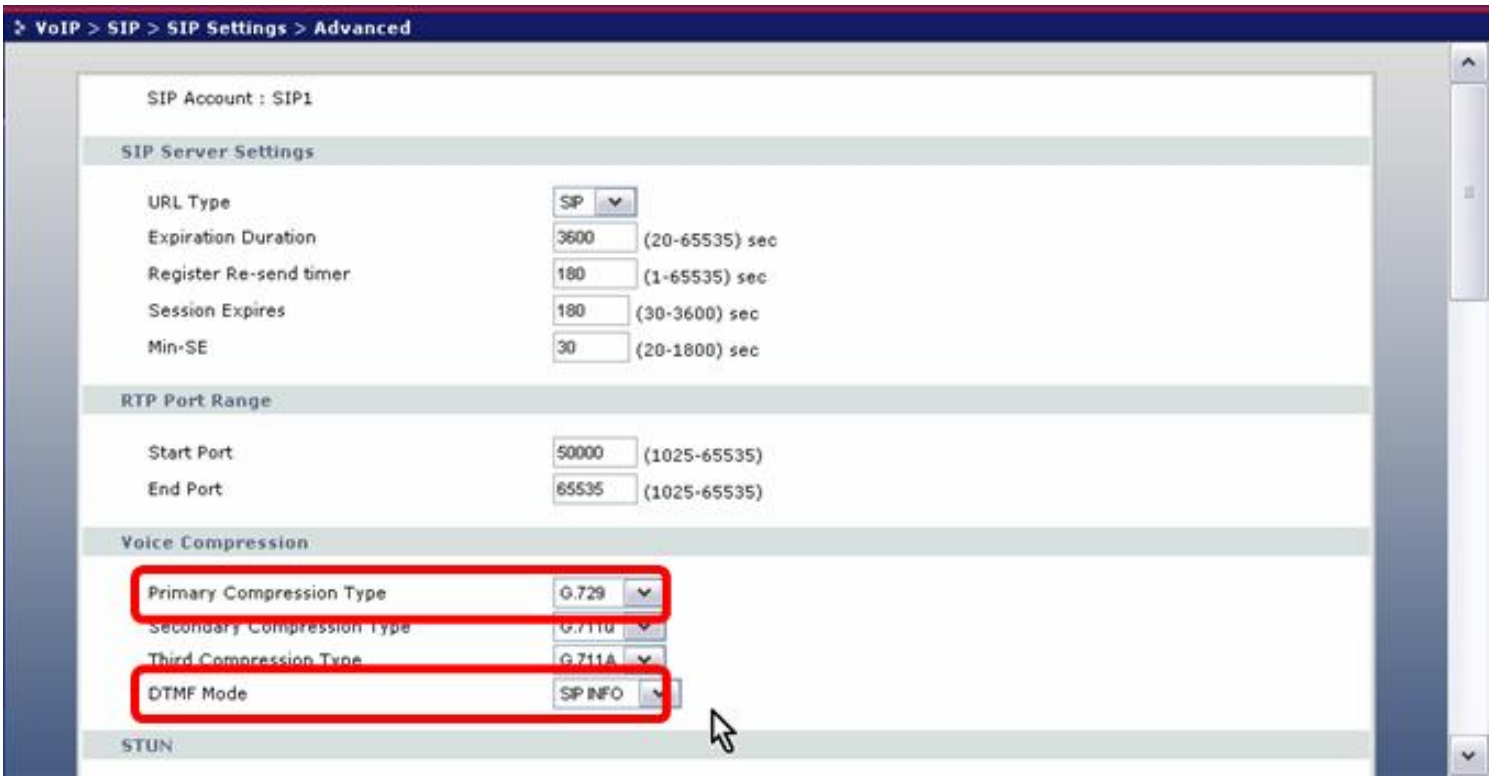
5. You and the remote MSN user can start communicating with each other with instant text messaging and video display.



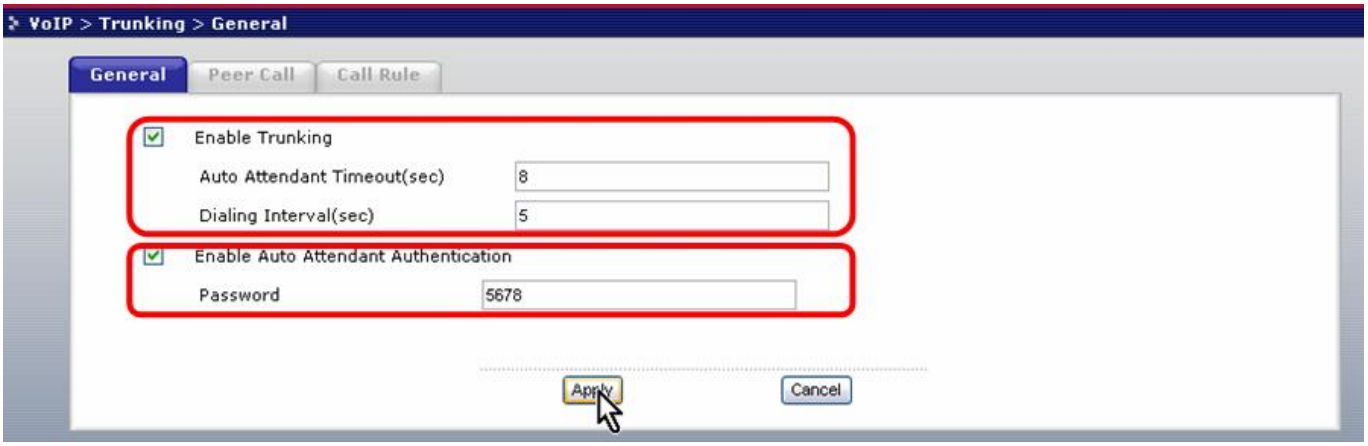
Trunk Setup in P-2302HWL/HWUDL-P1

- **Follow the 3 steps below to set up trunks on P-2302HWL/HWUDL-P1.**
  - Step 1: Connect the ports (WAN, LAN, Lifeline and FXS) on P-2302HWL/HWUDL-P1. Then turn on the device.

- Step 2: Access the web configurator and click VoIP > Advance Setting.
  Select the "primary compression to G.729" and "DTMF mode to SIP info" options.



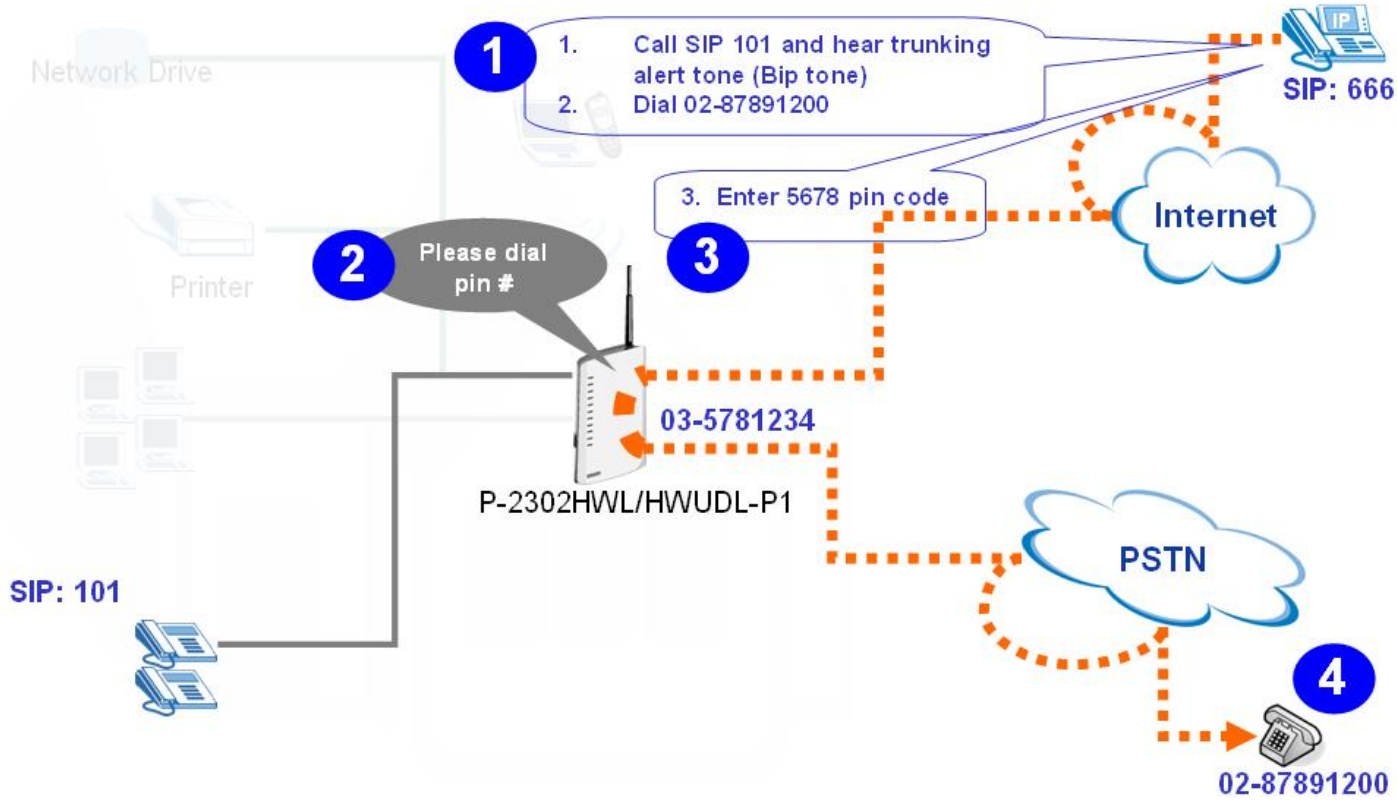
- Step 3: Click VoIP > Trunking and select to enable trunking. You can also enable auto attendant authentication if pin code authentication is required before using the trunk.



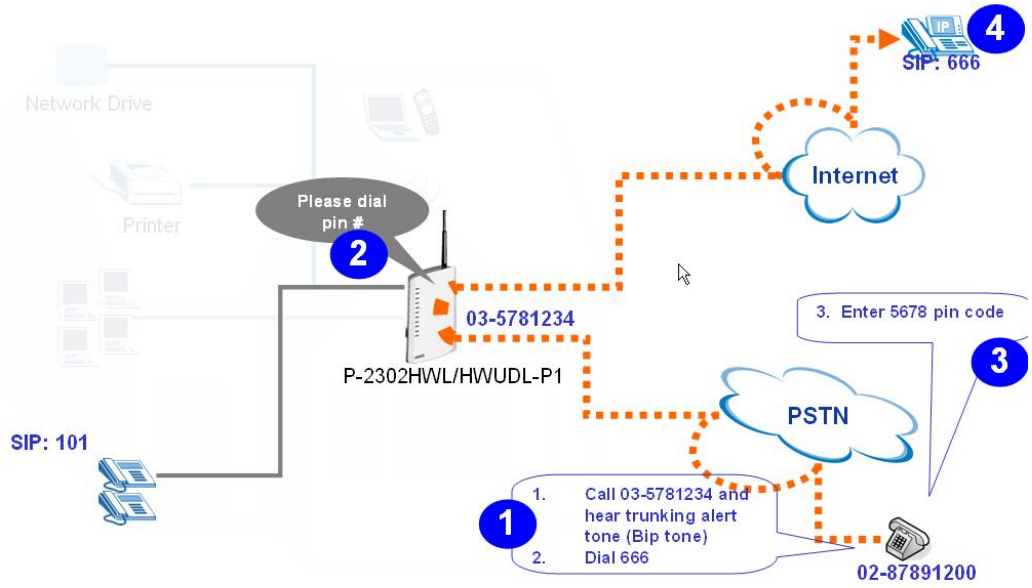
So how do you make a phone call over the PSTN and SIP networks?

Two examples are described next.

Example 1:
To make phone call over the PSTN and SIP networks, enter the pin code if required. SIP initiates the call and forwards it to PSTN.



Example 2:
To make a phone call over PSTN and SIP networks, enter the pin code if required. PSTN initiates the call and forwards it to SIP.



VoIP Application Notes

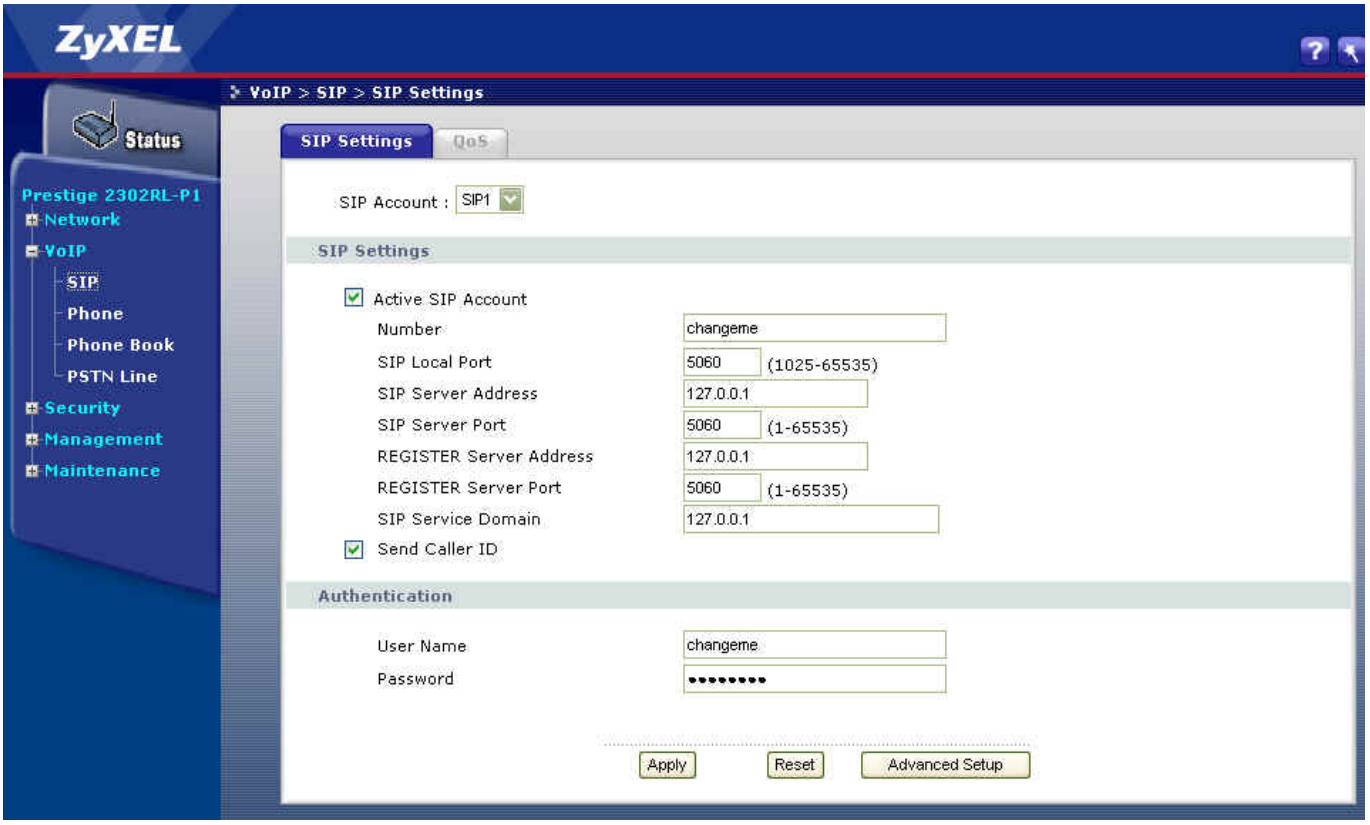
SIP Account Setup

VoIP is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network.

Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

The Prestige supports up to two SIP accounts simultaneously. Follow the procedure below to configure SIP accounts on the device.

Note: You should have a voice account already set up and have VoIP information from your VoIP service provider prior to configuring a SIP account on the Prestige.



After you have obtained the account information your ITSP provider provided, you can start configuring the SIP account.

Step 1. Log into the web configurator on the Prestige. Open a web browser and enter the management IP address (the default is 192.168.1.1) as the URL.

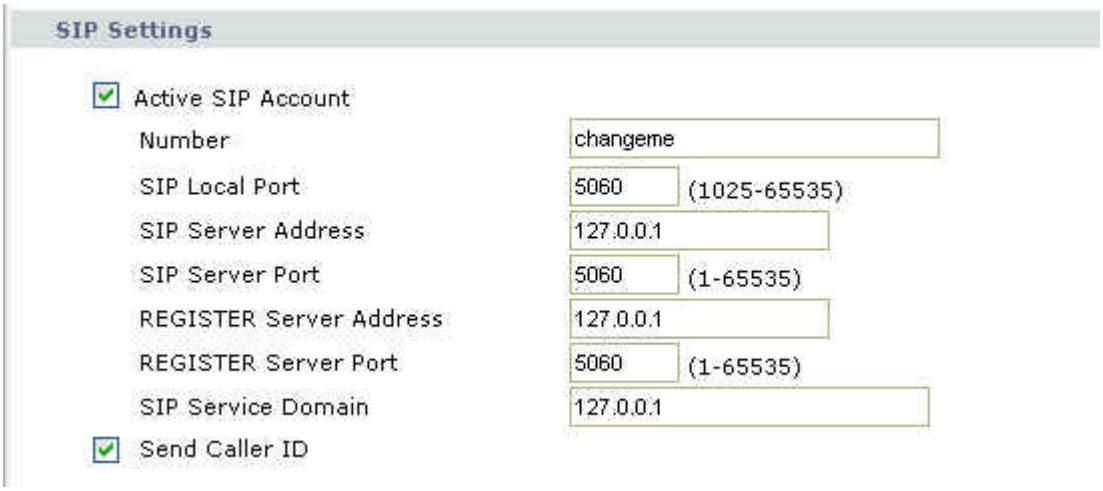
Step 2. A login screen displays. Enter the administrative login password (the default is **1234**).

Step 3. In the main menu, click **VoIP > SIP** to display the **SIP Settings** screen. In the **SIP Account** drop-down list box, select a SIP account you want to configure.

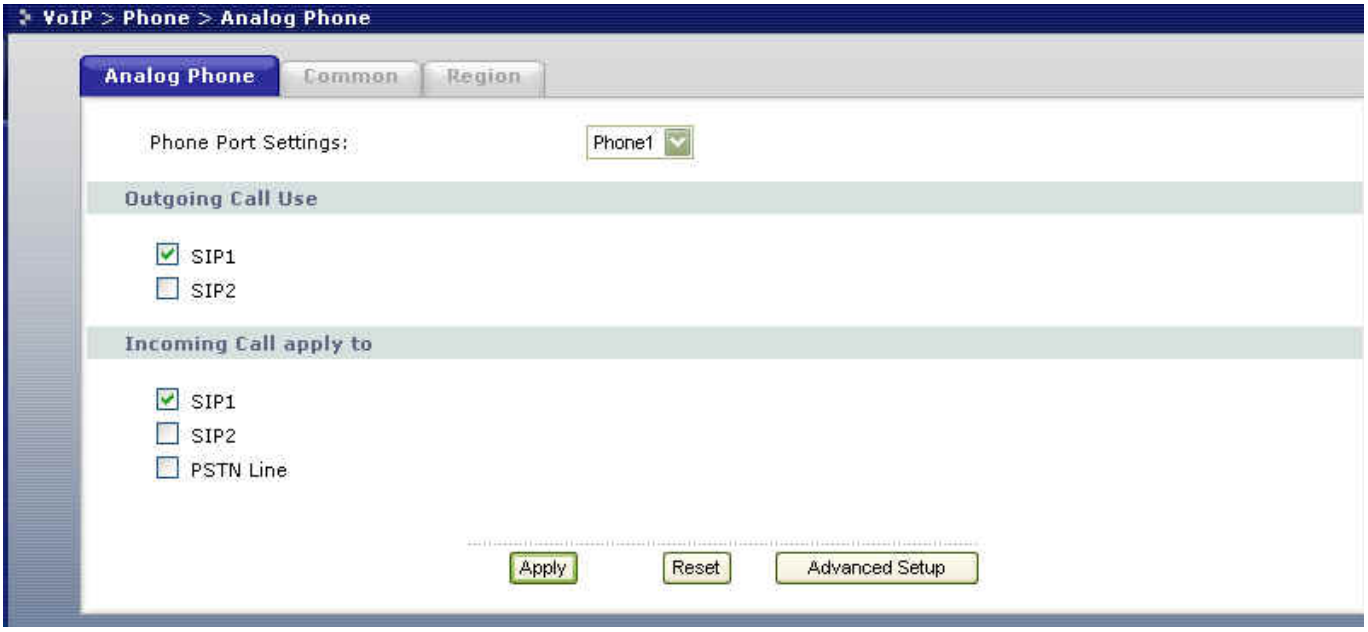
Step 4. Select **Activate SIP Account** to enable this account and set the account information (such as **SIP number, SIP local port, SIP server address, SIP server port, Register server port, Register server address, SIP service domain**) in the fields below. Your ISP should provide you with the account information.

Step 5. Under **Authentication**, enter the account user name and password exactly as given by your ISP.

Step 6. Under **SIP Settings**, select **Send Caller ID** if you want to send the caller ID. Otherwise, clear the check box.



Step 7. You associate the SIP account to a specified phone port on the ZyXEL device. This allows you to set which phone(s) to use (ring) when an incoming call is received. In the WEB GUI, click **VoIP > Phone** to display the **Analog Phone** screen. Select a phone index number in the **Phone Port Settings** field and select which SIP account to use in the **Outgoing Call Use** section.



Step 8. Click on **Apply** to save the changes and make the settings take effect. If you want to configure the second SIP account, select **SIP2** in the **SIP Account** field and follow steps 1 – 7.

Note: If you associate both phone ports are associated with both SIP accounts, you cannot identify which account's incoming call is received.

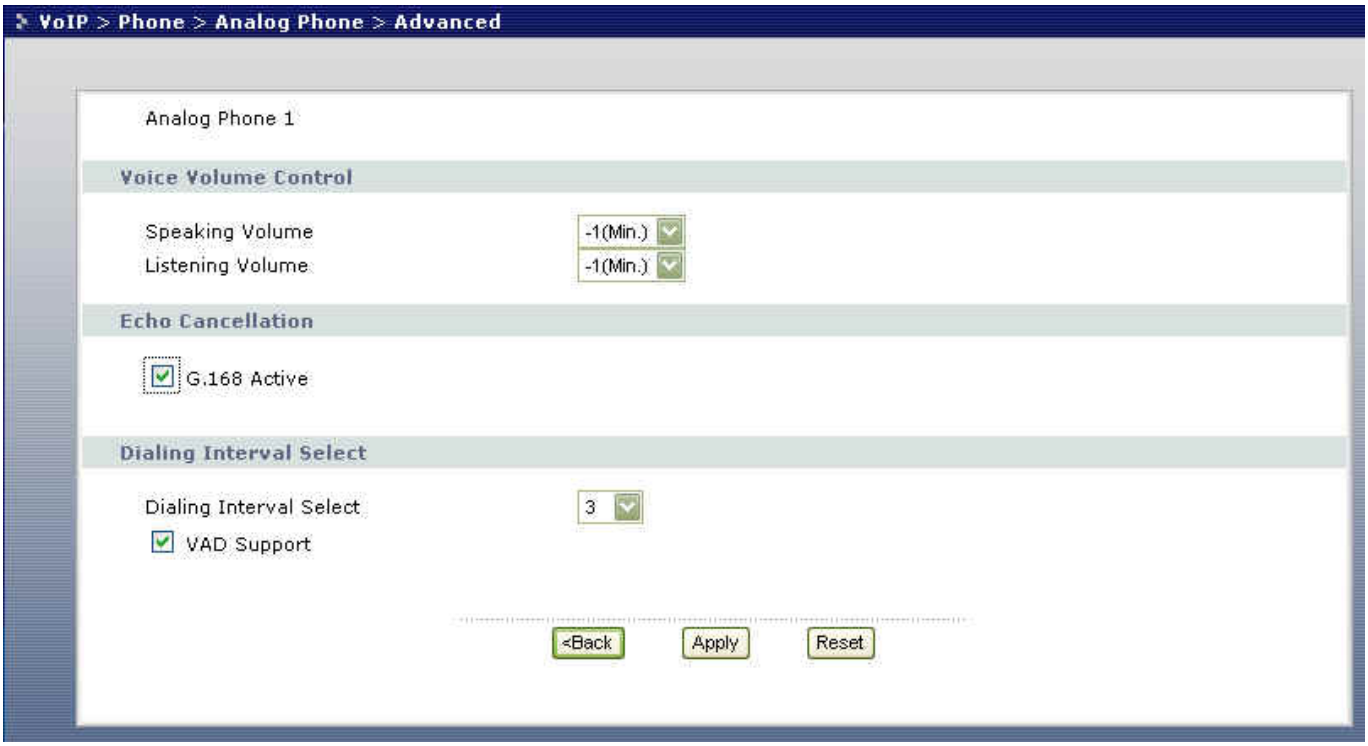
The following table describes the screen labels.

Label	Description
SIP Account	You can configure the Prestige to use multiple SIP accounts. Select one to configure its settings on the Prestige.
SIP Number	A SIP account's Uniform Resource Identifier (URI) identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. It is also known as a SIP identity or address. The format of a SIP identity is SIP-Number@SIP-Srevice-Domain. A SIP number is the part of the SIP URI that comes before the "@" symbol. Enter your SIP number in this field. You can use up to 31 ASCII characters.
SIP Local Port	Use this field to configure the Prestige's listening port for SIP. Leave this field set to the default if you were not given a local port number for SIP.
SIP Server Address	Type the IP address of the SIP server in this field.
SIP Server Port	Enter the SIP server's listening port for SIP in this field. Leave this field set to the default if your VoIP service provider did not give you a local port number for SIP.
REGISTER Server Address	A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register. Enter the SIP register server's address in this field. **If you were not given a register server address, then enter the address from the** SIP Server Address **field again here.**
REGISTER Server Port	Enter the SIP register server's listening port for SIP in this field. **If you were not given a register server port, then enter the port from the** SIP Server Port **field again here.**
SIP Service Domain	A SIP service domain is the domain name that comes after the @ symbol in a full SIP URI. Enter the SIP service domain name in this field. You can use up to 127 ASCII Extended set characters.

Authentication User ID	This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. Use ASCII characters.
Authentication Password	Type the password associated with the user name above. Use ASCII Extended set characters.
Block Caller ID	Select this check box to not show identification information when you make VoIP calls. Clear this check box to show identification information when you make VoIP calls.
Apply to	**Phone 1** and **Phone 2** correspond to the Prestige's physical **PHONE 1** and **2** ports, respectively. Select whether you want to receive calls for this SIP account on **Phone 1**, **Phone 2** or both. If you select both, you will not know which SIP account a call is coming in on.
Advanced Settings	Click **Settings** to open a screen where you can configure the Prestige's advanced VoIP settings like SIP server settings, the RTP port range and the coding type.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

Advanced Phone port settings

You can configure the ring/speaker volume and the echo cancellation settings for each phone port on the Prestige.



To configure advanced phone port setting, follow the steps below.

Step 1. Access the web configurator on the Prestige. In a web browser, enter the management IP address (the default is 192.168.1.1) of the Prestige in the address bar.

Step 2. A login screen displays, enter the administrative login password (the default is **1234**).

Step 3. In the navigation panel, click **VoIP > Phone > Analog Phone**.

Step 4. In the **Phone Port Settings** field, select which phone port you want to configure and click **Advanced Setup**.

Step 5. Set the phone port parameters and click **Apply** to save the settings and make the changes take effect. If you want to configure the second phone port, select **SIP2** in the **SIP Account** field and follow steps 1 – 5.

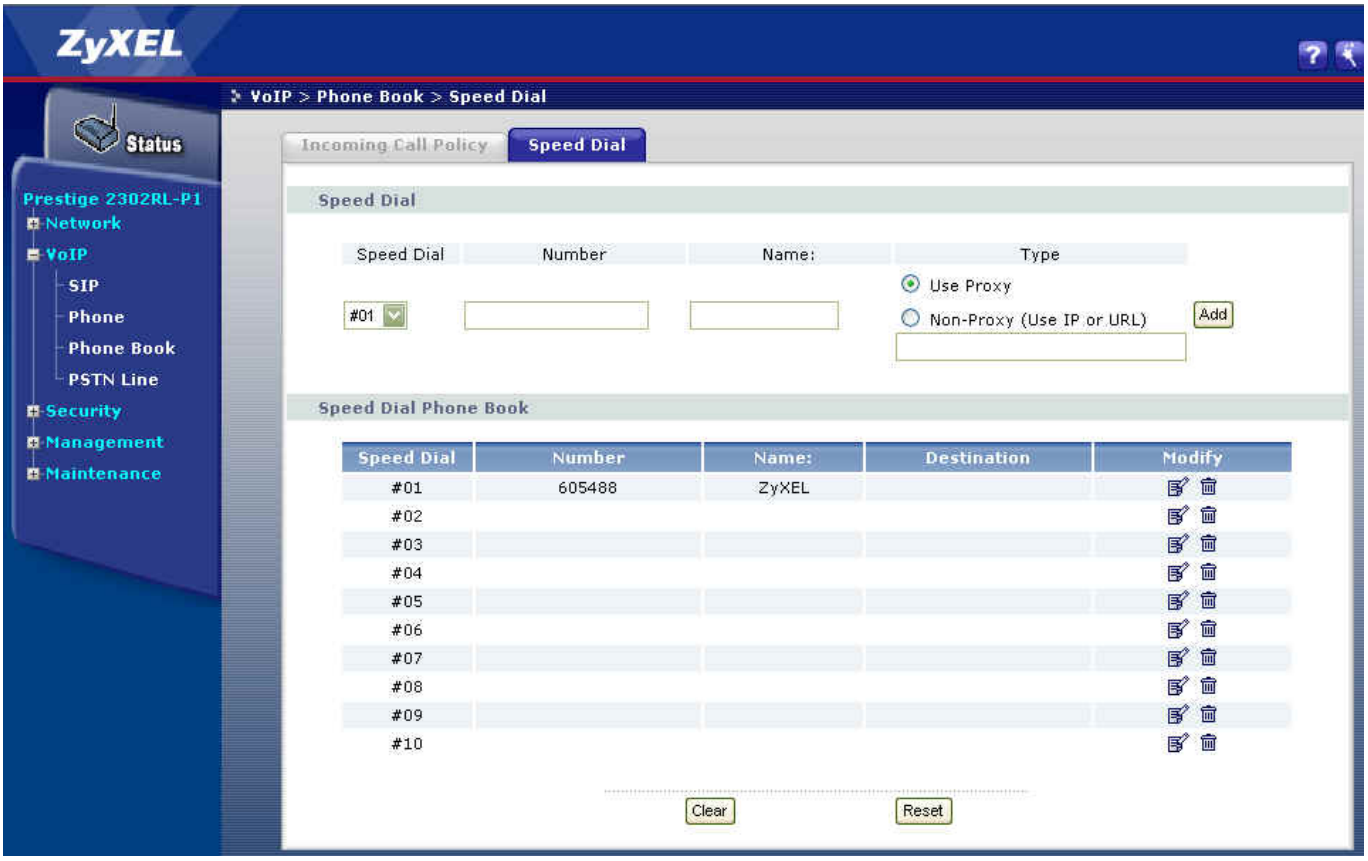
The table below describes the related fields.

Label	Description
Phone Port Settings	Use this field to select the phone port that you want to configure.

Speaking Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it sends to the peer device. -1 is the quietest and 1 is the loudest.
Listening Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it receives from the peer device and sends to your phone. -1 is the quietest and 1 is the loudest.
Outgoing Call use	**SIP 1** and **SIP 2** correspond to the Prestige's SIP accounts. Select whether you want the phone(s) attached to this phone port to use SIP account 1, 2 or both when you make a call. If you select both SIP accounts, the Prestige will first try to use SIP account 2 and then SIP account 1 when you make a call.
G.168 Active	Select this check box to cancel the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
VAD Support	Select this check box to use Voice Activity Detection (VAD) to reduce the bandwidth that a call uses. The Prestige will generate and send comfort noise when you are not talking.
Dialing Interval	When you are dialing a telephone number the Prestige waits this long after you stop pressing the buttons before initiating the call. Select how many seconds you want the Prestige to wait after the last input on the telephone's keypad before dialing (making) a call.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

Speed dial Phone book setup

You can configure up to 10 SIP phone number in the Prestige' s phone book for speed dialing.



Follow the steps below to configure the speed dial phone book.

Step 1. Access the web configurator on the Prestige. In a web browser, enter the management IP address (the default is 192.168.1.1) of the Prestige in the address bar.

Step 2. A login screen displays, enter the administrative login password (the default is **1234**).

Step 3. In the navigation panel, click **VoIP > Phone Book > Speed Dial** to display the configuration screen

Step 4. Select a speed dial key combination you want to configure in the **Speed Dial** column.

Step 5. In the **Number** field, enter the SIP number of the remote party. In the **Name** field, enter a description for the number. Then select **Use Proxy** or select **Non Proxy** and enter the static IP address or URL of the remote peer.

Step 6. Click **Add** to save the entry to the phone book.

Each field's detail description of the page is listed below.

Label	Description
Add New Entry	Use this section of the screen to edit and save new or existing speed dial phone book entries.
Speed Dial	Select a speed dial key combination from the drop-down list box.
SIP Number	Enter the SIP number of the party that you will call (use the number or text that comes before the @ symbol in a full SIP URI). You can use up to 127 ASCII characters.
Name	Enter a descriptive name to identify the party that you will use this entry to call. You can use up to 127 ASCII characters.
Type	Select **Use Proxy** if calls to this party use your SIP account configured in the VoIP screen. Select **Non-Proxy (Use IP or URL)** if calls to this party use a different SIP server or go directly to the callee's VoIP phone (IP-to-IP). Enter the SIP server's or the party's IP address or domain name (up to 127 ASCII Extended set characters).
Add	Click this button to save the entry in the speed dial phone book. The speed dial entry displays in the **Speed Dial Phone Book** section of the screen.
Speed Dial Phone Book	This section of the screen displays the currently saved speed dial entries. You can configure up to 10 entries and use them to make calls.
Speed Dial	This is the entry's speed dial key combination. Press this key combination on a telephone attached to the Prestige in order to call the party named in this entry.
Name	This is the descriptive name of the party that you will use this speed dial entry to call.
SIP Number	This is the SIP number of the party that you will call.
Type	This field displays **Use Proxy** if calls to this party use one of your SIP accounts. This field displays the SIP server's or the party's IP address or domain name if calls to this party do not use one of your SIP accounts.
Delete	Click this button to remove an entry from the speed dial phonebook.
Edit	Click this button to change the speed dial entry. The speed dial entry displays in the **Add New Entry** section of the screen where you can edit it.

Clear	Click this button to remove all of the entries from the speed dial phonebook.

FAQ

ZyNOS FAQ

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 and public download web site as they become available.

How to access the embedded web configurator?

The web configurator is a user friendly configuration interface via a web browser. You can access the web configurator by entering the LAN IP address of the Prestige in the web browser. The default the Prestige LAN IP is 192.168.1.1. Your computer IP address must be in the same subnet (or range) as the Prestige's LAN IP address.

What is the default LAN IP address and password? And, how do I change it?

The default LAN IP address is "192.168.1.1" and you can change the LAN IP in web configuration (click LAN > LAN TCP/IP). The default login password is 1234. After you have successfully logged into the web configuration, you can change the password in the Password screen (click SYSTEM > Password. In the Password screen, enter the old password and the new password and the new password again to confirm. Click Apply to save the changes.

How do I upload the firmware via the web configurator?

Follow the procedure below to update the device firmware via the web configurator.

a. Log into the web configurator.
b. In the navigation panel, click MAINTENANCE.
c. Click the F/W Upload tab.
d. Click Browse and locate the directory of the firmware you want to upload and click Upload.
e. A message displays indicating that the firmware is successfully updated and that the Prestige will reboot.

How do I upgrade/back up the firmware using an FTP client program through the LAN?

You can use an FTP program to transfer files (firmware or configuration files) to or from the Prestige. Follow the procedure below to upload the firmware to a device using FTP.

a. Use an FTP program to put the firmware file (rename as "ras") on the Prestige. After the file transfer is complete, the Prestige stores the uploaded firmware to its FLASH ROM and reboots.
   Note: Do NOT turn off the device while the file transfer process is in progress. Doing so will damage your device and render it useless. Wait until the system LED turns steady before accessing the device.
b. To backup your firmware, use the FTP client program to get the 'ras' file from the Prestige.

How do I upload or back up the configuration file (the ROM file) via the web configurator?

You can upload a configuration file to restore the device to the previously saved configuration, or reset the device to the factory defaults.

Follow the procedure below to upload a configuration file via the web configurator.

a. Log into the web configurator.
b. In the navigation panel, click MAINTENANCE.
c. Click the Configuration tab.
d. Click the Restore tab and click Browse o locate the directory of the configuration file you want to upload.
e. Click Upload.

Follow the procedure below to back up the configuration file from the device via the web configurator.

a. Log on into the web configurator.
b. In the navigation panel, click MAINTENANCE.
c. Click the Configuration tab.
d. Click Backup. A screen displays prompting you to specify a location to store the configuration file.
e. Click Save file and browse to where you want the file to be saved.
f. Click Save.

How do I back up/restore configurations using an FTP client program through the LAN?

a. Use an FTP client program in your computer (such as the Cuteftp or wsftp client) to log into your Prestige.
b. To back up current device configuration, use the FTP client program to get the 'rom-0' file from the Prestige.
c. To restore device configuration, use the FTP client program to put a configuration file (rename to ROM-0) on the Prestige.

Why can't I telnet into Prestige from the WAN?

The following lists the possible reasons why you cannot telnet into the Prestige from the WAN.

a. You did not enable the Telnet service on WAN interface for remote management in SMT menu 24.11.
b. Telnet service is enabled but your computer IP address is not included in the secured host list in SMT menu 24.11. In this case, you will see the 'Client IP is not allowed!' error message in the Telnet screen.
c. The default filter rule 3 (Telnet_FTP_WAN) is applied in the Input Protocol field in SMT menu 11.5. This blocks access from the WAN.

What should I do if I forget the system password?

In case you forget the system password. You can reset the unit back to the factory defaults. You can do this by using a sharp pointed object (such as a pen) to press and hold down the Reset button for 5 seconds or until the power LED starts to blink, then release. The unit is reset back to the factory defaults. The reset button is located near the power jack on the unit’ s back panel

Note: Resetting the unit back to the factory defaults erases all your previous settings.

What is SUA? When should I use SUA?

SUA (Single User Account) is a unique feature supported by the Prestige to allow more than one person to access the 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 recomputed the appropriate header checksums and forwards the packet to the Internet as if it originated from the Prestige using the WAN IP address assigned by the ISP. When reply packets from the Internet are received by the Prestige, the original IP source address and TCP/UDP source port numbers are written back 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 intended destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

What is the difference between NAT and SUA?

NAT is a generic name defined in RFC 1631 'The IP Network Address Translator (NAT)'. SUA (Internet Single User Account) is ZyXEL's proprietary implementation and trade name for the PAT feature which is a specific type of NAT. SUA (or PAT for NAT) translates address into port mapping.

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

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

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

How many network users does SUA/NAT support?

The Prestige does not limit the number of the users but the number of the sessions for Internet access. The Prestige supports 1024 sessions. You can view the current active sessions using the 'ip nat iface enif0 disp' command in SMT menu 24.8.

What are Device and Protocol filters?

In ZyNOS, there are two filter groups: device filter and protocol filter. Generic filters belong to the device filter group while TCP/IP and IPX filters belong to the protocol filter group.

Why can't I configure device or protocol filters?

In ZyNOS, you cannot configure device filters and protocol filters in the same filter set.

Product FAQ

What is the Prestige Internet Access Sharing Router?

The Prestige series meets the requirements of most network environments, from small and medium businesses, SOHO, Telecommuters, to home user or education applications. Prestige is designed to help users save expenses, minimize maintenance, and simultaneously provide a high-quality networking environment. In addition, the Prestige provides secure network connection with a firewall and IPSec VPN.

The Prestige series is a robust solution complete with everything needed for providing Internet access to multiple workstations through your cable or ADSL modem. The router is equipped with 2 auto-MDI/MDIX 10/100Mbps Ethernet WAN ports, 1 auto-MDI/MDIX 10/100Mbps Ethernet LAN port, 4 auto-MDI/MDIX 10/100Mbps DMZ ports and IEEE 802.11b wireless capability. It is the cost-effective solution that provides easy-to-setup Internet connection and IEEE 802.11 wireless connectivity for multiple users.

Numerous popular Internet applications (such as Web, E-Mail, FTP, Telnet, Gopher) are supported. The Prestige is designed for SOHO, branch offices, workgroups, and educational users.

Will the Prestige work with my Internet connection?

The Prestige is designed to work with cable and ADSL modems. The Prestige comes with an Ethernet port to connect to your computer so the Prestige is placed between your computer and your modem. The Prestige also supports PPPoE Internet connection type.

What do I need to use the Prestige?

Ethernet ports for LAN and WAN connection. You should connect the computer to the LAN port and the external modem to the WAN port. If the ISP uses PPPoE or Roadrunner Authentication, you need the user account to enter in the Prestige.

What is PPPoE?

PPPoE (Point-to-Point Protocol over Ethernet) is an IETF draft standard specifying how a computer interacts with a broadband modem (such as xDSL, cable, wireless, etc.) to access the high-speed data networks via a PPP dialer (such as Microsoft' s Dial-Up Networking). PPPoE supports a broad range of applications and services including authentication, accounting, secure access and configuration management. Some ISPs still provides PPPoE connection type today. Before configuring PPPoE in the Prestige, make sure your ISP supports PPPoE.

Does the Prestige support PPPoE?

Yes. The Prestige has already supported PPPoE since ZyNOS 2.50.

How do I know I am using PPPoE?

PPPoE requires a user account to log into the service 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 connect to the Internet when you turn on your computer, you probably are not using PPPoE. You can also check with your ISP or the information sheet given by the ISP. Choose PPPoE as the encapsulation type in the Prestige if the ISP uses PPPoE.

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 services including authentication, accounting, secure access and configuration management.

Which Internet Applications can I use with the Prestige?

The Prestige supports most common applications including MIRC, PPTP, ICQ, Cu-SeeMe, NetMeeting, IP/TV, RealPlayer, VDOLive, Quake, QuakeII, QuakeIII, StarCraft, and Quick Time.

How can I configure the Prestige?

a. Telnet remote management- Menu driven user interface for easy remote management

b. Web browser- embedded web server for easy configuration

What network interface does the Prestige support?

The Prestige comes with a 10/100M Ethernet interface to connect to your LAN computer and the external cable/DSL modem.

What can I do with the Prestige?

You can connect to the Internet through the Prestige. This allows you to browse the web, send and receive e-mail, and download/share files. These are just a few of many benefits you get when you put the whole office on-line with the Prestige Internet Access Sharing Router.

Does the Prestige support dynamic IP addressing?

Yes. You can set the Prestige to use a static WAN IP address or set it to use a dynamic IP address from the ISP.

What is the difference between the internal IP and the real IP from my ISP?

Internal IP addresses are also referred to as virtual IP addresses. They are a group of up to 255 IP addresses that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP address (or the public IP address) you obtain from the ISP, instead, can be recognized or pinged by other real IP addresses. The Prestige Internet Access Sharing Router works like an intelligent router that routes network traffic between the virtual IP addresses and real IP addresses.

How does e-mail work through the Prestige?

It depends on what kind of IP address you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through the Prestige using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access rights.

If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address.

Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through the Prestige using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access rights.

What is the difference between the 'Standard' and 'RoadRunner' service?

The Road Runner service is commonly used in the USA and it requires the user to "log in" to the service provider network before Internet access is allowed. The most popular implementation is TAS (Toshiba Authentication System) with a packet filtering firewall in the upstream direction. Before users are logged in, they can send ICMP packets (that is, ping) to a remote host through the Internet. However, all outgoing (upstream) TCP and UDP packets to the Internet are blocked. Thus users can access the local local DNS/login server. Downstream packets (or packets from the Internet to the users) are not filtered or blocked.

With Standard service, no user login is required. This is commonly used with a cable modem. The Prestige supports both Road Runner and Standard services in SMT menu 4 for connecting to the ISPs for Internet connection.

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

Yes, it is possible because Prestige 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 SMT Menu 15 - SUA Server Setup.

What DHCP capability does the Prestige support?

The Prestige supports DHCP client on the WAN port and DHCP server on the LAN port. The Prestige's DHCP client allows it to get a public WAN IP address from the ISP automatically if your ISP uses DHCP as a method to assign IP addresses. The Prestige's internal DHCP server allows it to automatically assign IP and DNS server addresses to clients on the local LAN.

How do I use the reset button? And which parameter will be reset by the reset button?

Use a sharp pointed object to press the reset button located near the power connector. Press and hold down the button for about five seconds to reset the device. All device settings, including the login password and IP address, will be reset to the factory defaults.

The default IP address is 192.168.1.1 and the default login password is 1234.

What network interface does the new Prestige series support?

The new Prestige series comes with an auto MDX/MDIX 10/100M Ethernet LAN port to connect to computer(s) or switch(es) on the LAN and one 10/100M Ethernet port to connect to the external cable/DSL modem on the WAN.

Does the Prestige support TFTP?

Yes. In addition to the direct console port connection, the Prestige supports firmware upload and configuration file uploading/download using TFTP (Trivial File Transfer Protocol) over LAN.

Does the Prestige support TFTP over WAN?

Although TFTP also works over the WAN, it is not recommended because of potential data corruption error while transferring files to the Prestige.

How can I upload data to outside Internet over the one-way cable?

Set up an alternate path for connection to the Internet (for example, a dialup connection). You can still receive downstream packets from the Internet through the Prestige.

How fast is the DSL connection?

There are a number of factors that can affect the speed of your ADSL connection. The connection speed may depend on how fast your computer handles data, how fast data can be transmitted between your computer and the modem, how well the cable modem handles traffic during network congestion, or how much bandwidth is provided by the ISP, etc.

Depending on your computer, data process speed varies and few computers can achieve data processing rates at up to 30 Mbps.

Ethernet (10baseT) is the most popular cable modem interface standard for a computer. This automatically limits the speed of the connection to less than 10 Mbps even if the modem can receive at 30 Mbps. Most Local Area Networks use 10baseT Ethernet, and although they are 10 Mbps networks, it takes a much longer than one second to transmit 10 megabits (or 1.25 megabytes) of data from one terminal to another.

Cable modems on the same node share the same bandwidth, which means that congestion is created when too many people try to access the Internet at the same time. In addition, when one user is downloading large graphic

or video files, a significant portion of the shared bandwidth is used thus slowing down access for other users in the same neighborhood.

Most independent Internet Service Providers today connect to the Internet using a single 1.5 Mbps "T1" telephone line. All their subscribers share that 1.5 Mbps bandwidth. Cable companies connecting to the Internet backbone using a T1 limit their subscribers to an absolute maximum of 1.5 Mbps.

To create the appearance of faster network access, ISPs store or "cache" frequently requested web sites and Usenet newsgroups on a server in the central office (CO). Storing data locally will remove some of the bottleneck at the backbone connection.

How fast can they go? Theoretically, they can receive data at speeds up to 30 Mbps. In the real world, with cost conscious cable companies running the systems, the speed will probably fall to about 1.5 Mbps.

My Prestige cannot obtain a WAN IP address from the ISP to connect to the Internet, what should I do?

There are various ways your ISP controls user access and login. Once a user has successfully logged into, the ISP will provide the WAN IP address to the user.

The following lists the methods ISP’ s authenticates users.

1. Check if the modem’ s MAC address' is valid.
2. Check if the host name is correct. The host name is usually the text after the @ sign. For example, @home
3. Check if the user ID is valid. This is commonly used with the RR-Toshiba Authentication and RR-Manager Authentication services.

If you are not able to get a WAN IP address from your ISP, check which authentication method your ISP uses and configure the settings on the Prestige. The following sections describe how you can solve this problem.

1. If your ISP checks the MAC address

Some ISPs checks the user device (usually a computer) MAC address before assigning a WAN IP address. If the MAC address matches one on the ISP’ s system, the ISP sends an IP address to the user device and allows Internet access. However, if the user connects another computer with a different MAC address directly to the modem, the ISP discards any DHCP discovery packets from the un-authorized MAC address and no IP address is assigned.

You can set the Prestige to copy the MAC address of the computer whose MAC address is authorized by the ISP. The Prestige will use the copied MAC address as its WAN MAC address.

In SMT menu 2, enter the computer MAC address. The Prestige will use the copied MAC address as its WAN MAC address and update SMT menu 24.1.

```
MAC Address:
Assigned By= IP address attached on LAN
IP Address= 192.168.1.33
```

Field settings:

a. Assigned By: Select IP address attached on LAN.
b. IP Address: Enter the IP address of the computer whose MAC address is authorized by the ISP.

2. If your ISP checks the host name

Some ISPs checks the host name information contained in the DHCP request sent by the user computer. A host name is text that comes after the @ sign. For example, in account@home.com, the host name is "home.com". If a technician from your ISP helped you set up Internet connection, he/she set the host name as the computer name on your computer (in the Networking screen). When you connect that computer to the Prestige, you must set the same name as the Prestige's system name in SMT menu 1.

```
Menu 1 - General Setup

System Name= zyxel
```

Field Setting:

- System Name: Enter the same name as the computer.

3. If your ISP checks the User ID

This authentication method is used mostly by ISPs providing RoadRunner services (for example, RR-TAS (Toshiba Authentication Service) or RR-Manager authentication). You must configure the service type, username and password exactly as provided by your ISP in SMT menu 4.

```
        Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
  Service Type= RR-Toshiba
  My Login= cso@zyxel
  My Password= ********
  Retype to Confirm= N/A
  Login Server= 0.0.0.0

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only
```

Field settings:

a. Service Type: Select **RR-TAS** or **RR-Manager** authentication method used by your ISP.
b. Login Server: Enter the IP address of the authentication server if you know it. Otherwise, leave this field to the default to have the Prestige automatically obtain this information.
c. My Login Name: Enter the login user name given to you by your ISP
d. My Password: Enter the password associated with the login name.
e. WAN IP Address Assignment: If the ISP did not assign you a fixed (or static) WAN IP address, select **Dynamic**, otherwise, select **Static**.
f. IP Address, Subnet Mask, Gateway IP Address: If you select **Static** in the **WAN IP Address Assignment** field, enter the IP address, subnet mask and gateway device IP address provided by your ISP.

What is BOOTP/DHCP?

BOOTP (Bootstrap Protocol) and DHCP (Dynamic Host Configuration Protocol) are mechanisms to dynamically assign an IP address to a TCP/IP client from the server. In this case, the Prestige Internet Access Sharing Router is a BOOTP/DHCP server. Windows clients use DHCP to request an internal IP address, while WFW and WinSock clients use BOOTP. TCP/IP clients may specify their own IPs or use BOOTP/DHCP to request an IP address.

What is DDNS?

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname, allowing your computer to be more easily assessable from various locations on the Internet. To use the service, you must first apply an account from one of the several free DDNS service providers such as WWW.DYNDNS.ORG.

Without DDNS, you have to tell your users the WAN IP address of your server for them to access. It is inconvenient for the users if this IP is dynamic which changes. With DDNS supported on the Prestige, you use a DNS name (e.g., www.zyxel.com.tw) supplied by the DDNS service provider to your server (e.g., Web server). Outside users can always access the web server at www.zyxel.com.tw regardless of whether the WAN IP on the Prestige is dynamic or static.

When the ISP assigns the Prestige a new IP address, the Prestige updates this IP address to the 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 easily accessible.

When do I need the DDNS service?

When you want your internal server to be accessible by using DNS name rather than using a dynamic IP address, use the DDNS service. The DDNS server maps a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP address, the Prestige sends this IP address to the DDNS server to update its IP-DNS table.

What DDNS servers does the Prestige support?

Currently, the Prestige supports WWW.DYNDNS.ORG for DDNS service. This is the web site to which you apply the DNS and update the Prestige WAN IP.

What is DDNS wildcard?

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

Does the Prestige support DDNS wildcard?

Yes. the Prestige supports DDNS wildcard that WWW.DynDNS.ORG supports. To use wildcard, simply enter yourhost.dyndns.org in the Host field in SMT menu 1.1.

Can VPN tunnels still work on a Prestige using SUA?

Yes, the Prestige's SUA still works in IPsec ESP Tunneling mode. When packets go through the Prestige, SUA will translate the source IP address and source port for the host. To forward IPsec packets, the Prestige SUA can identify ESP packets with a protocol number of 50. Thus SUA will replace the source IP address of the IPsec packet with the router's WAN IP address. However, SUA will not change the source port of the UDP packets which are used for key managements. Since the remote gateway checks the actual source port during connection negotiation, SUA should not change the original source port.

How do I set up my Prestige to route IPsec packets over SUA?

For outgoing IPsec tunnels, no extra setting is required. To forward packets through the inbound IPsec ESP tunnel, you must configure the 'Default' server set in SMT menu 15. It is because SUA makes your LAN appear as a single device to the outside world. LAN users are invisible to outside users. So, to make an internal server accessible from the outside, you must specify the service port and the LAN IP address of the internal server in SMT menu 15. Thus Prestige is able to forward incoming packets to the requested service behind SUA and the outside users can access the server using the Prestige's WAN IP address. You must configure the internal IPSec gateway as the default server (unspecified service port) in SMT menu 15.

VoIP FAQ

What is Voice over IP?

Voice over IP (VoIP) is an emerging technology based on the open IEEE standards. VoIP refers to the transmission of voice data over the Internet. Various protocols are available for voice transport. The most commonly used are SIP and H.323.

Voice over IP (VoIP) is an emerging technology based on open IEEE standards. VoIP refers to the transmission of voice data over the Internet. Various protocols are available for voice transport. The most commonly used are SIP and H.323.

How does Voice over IP work?

In VoIP, voice data is sent digitally in discrete packets through the Internet, not through the traditional circuit switch of PSTN. To do so, an analog-to-digital converter is required at sender side to translate voice (analog signal) to digital signal before transmission. At the receiver end, an analog-to-digital converter converts the digital signal back to analog so the voice can be heard on the phone.

Why use VoIP?

Traditionally voice data is transmitted using circuit switching. Since circuit switching is designed to carry voice, it does it very well. However, as broadband networks become a mainstream for network access and technologies have evolved, we don't want to confine ourselves to just using text-based applications (such as e-mail, instant messaging, etc.) for communication over the Internet. Thus, the convenience of voice communication through the Internet has quickly become popular.

In addition, it would take a much longer time, more effort and money to implement new features using circuit switching. Since the IP technology is a standard and various applications are available, it is easier and more cost-effective to integrate new services and applications using IP.

What is the relationship between codec and VoIP?

In order to send voice (analog signal) over IP, it first needs to be digitized. Codec is a technique used to digitize analog signal into digital signals and vice versa. There are various speech codec available for VoIP. Each codec has its advantages and disadvantages.

What advantage does Voice over IP provide?

VoIP provides advanced integration of text, video and voice in emails. This cannot be done using traditional circuit switching (PSTN).

What is the difference between H.323 and SIP?

H.323 and SIP are proposed by different groups. Session Initiation Protocol (SIP) is a standard introduced by the Internet Engineering Task Force in 1999 to carry voice over IP. Since it was created by the IETF, it approaches voice and multimedia from the Internet, or IP. Whereas H.323 emerged around 1996, and as an

International Telecommunication Union standard, it was designed from a telecommunications perspective. Both standards have the same objective - to enable voice and multimedia convergence with IP protocols.

Can H.323 and SIP interoperate with each other?

In interoperability between the two, the industry is making slow but sure progress. Interoperability must first happen between vendor implementations of the same protocol (SIP-to-SIP and H.323-to-H.323) and then between protocols. Currently in order for SIP client to talk to H.323 client the ITSP must have a trunking gateway act as a translator between the two protocols without the truncking gateway the two protocols are not able to communicate to one another.

What is voice quality?

Voice quality is how well a person can hear the voice on the opposite end.

How are voice quality normally rated?

Voice quality is most commonly rated through a voice quality metric called the Mean Opinion Score (MOS) which is recommendation by ITU-T. The MOS is a 5-point scale where 5 represent excellent voice quality and 1 represent bad voice quality.

What is codec?

Codec is an algorithm that converts analog signal into digital signal and vice versa. There are three codeec types: waveform, source, and hybrid codec. Each consume different amount of bandwidth and provide different voice quality.

What is the relationship between codec and VoIP?

VoIP is the general term to refer to the sending of digitized voice information in discrete packets over public digital network (the Internet) where other data packets can be sent at the same time. A codec determines how much bandwidth voice packets will use. To save bandwidth usage, you would use as little bandwidth as possible at the cost of reduced voice quality.

What codec types does Prestige support?

The Prestige supports the following commonly used codecs.

- G.729 voice codec
- G.711u-law voice codec

- G.711a-law voice codec

Which codec should I choose?

Choose a codec that is also supported on the remote VoIP host since both ends of the VoIP connection must use the same codec. In general, a codec with low bandwidth consumption and high voice quality is a good codec.

What do I need in order to use SIP?

The following lists the minimum requirement for running VoIP applications.

1. A high-speed Internet connection. You can connect to the Internet using a cable or DSL modem. Or subscribe to high-speed network services such as ISDN, DSL or T-1. The bandwidth requirement varies depending on the amount of traffic in your network.

2. A PC with VoIP software installed or an external VoIP gateway (such as an ATA or the Prestige 2602 VoIP station router).

3. An account from a VoIP services provider (such as an ITSP). The account can be configured to recognize your calls automatically, or you can require the users to enter their assigned unique account numbers.

I am unable to register to a SIP server

If you are unable to register to a SIP server, do the following.

1. Make sure the Internet connection is up and that you are able to ping the SIP register server from the LAN behind the Prestige. If your register server uses a domain name, make sure DNS name can be resolved. If you are using a static WAN IP address, make sure the DNS server is configured correctly on your Prestige.

2. Make sure the SIP account is correct and the password is entered correctly. They may be case-sensitive.

3. Check if there is a NAT router install before the Prestige which is a VoIP station gateway. It is NOT recommended that you install a NAT router in front of the Prestige as this may cause unexpected problems. If you still want to install a NAT router, use a VoIP ATA (VoIP Analog Telephone Adapter), such as the Prestige ATA series, instead.

I can register to the SIP server but cannot establish a call

If you are able to register to the SIP server but cannot make a call through the Prestige, it is very likely there a NAT router or a firewall blocks the traffic.

It is NOT recommended that you install a NAT router in front of the Prestige as this may cause unexpected problems. If you still want to install a NAT router, use a VoIP ATA (VoIP Analog Telephone Adapter), such as the Prestige ATA series, instead.

I can make or receive a call but the voice traffic only goes one way, not both way

If you can register to a server and can only make an out- going call but cannot receive incoming calls or the incoming call signal establishment can be made but the voice traffic only goes one way, there is very likely a NAT/firewall router installed before the Prestige. Refer to the NAT/firewall related questions for more information.

I have tried all the troubleshooting steps, but still cannot register to the SIP server. What should I do next?

In this case, contact your local service provider for support. If they cannot solve your problem, they will send your problem to the ZyXEL global technical support center. help out the problem they will escalate your problem to ZyXEL tech center.

To help us solve your problem quickly, please prepared the following information.

1. Serial number of the device.

2. SIP Call server type and service provider.

3. Your device firmware version and romfile (or the configuration file) with the administrator login password.

4. Detail information of what you have tried to resolve the problem.

What should I do if there may be a hardware problem with my Prestige?

Refer to the troubleshooting section in the user's guide for basic hardware troubleshooting and diagnostic tips. If the hardware problem persists after you have followed the User's Guide to remedy the problem, contact your ZyXEL local vendor and send the device in for service (with an RMA number).

Trouble Shooting

Unable to Get WAN IP from ISP

My Prestige cannot obtain an IP address from the ISP for Internet access, what should I do?

There are various ways your ISP controls user access and login. Once a user has successfully logged into, the ISP will provide the WAN IP address to the user.

The following lists the methods ISP’ s authenticates users.

4. Check if the modem’ s MAC address' is valid.
5. Check if the host name is correct. The host name is usually the text after the @ sign. For example, @home
6. Check if the user ID is valid. This is commonly used with the RR-Toshiba Authentication and RR-Manager Authentication services.

If you are not able to get a WAN IP address from your ISP, check which authentication method your ISP uses and configure the settings on the Prestige. The following sections describe how you can solve this problem.

---

1. If your ISP checks the MAC address

Some ISPs checks the user device (usually a computer) MAC address before assigning a WAN IP address. If the MAC address matches one on the ISP’ s system, the ISP sends an IP address to the user device and allows Internet access. However, if the user connects another computer with a different MAC address directly to the modem, the ISP discards any DHCP discovery packets from the un-authorized MAC address and no IP address is assigned.

You can set the Prestige to copy the MAC address of the computer whose MAC address is authorized by the ISP. The Prestige will use the copied MAC address as its WAN MAC address.

In SMT menu 2, enter the computer MAC address. The Prestige will use the copied MAC address as its WAN MAC address and update SMT menu 24.1.

```
                    Menu 2 - WAN Setup

              MAC Address:

                Assigned By= IP address attached on LAN

                IP Address= 192.168.1.33
```

Field settings:

- Assigned By=, Select **IP address attached on LAN.**
- IP Address=, Enter the IP address of the computer whose MAC address is authorized by the ISP.

---

2. If your ISP checks the Host Name

Some ISPs checks the host name information contained in the DHCP request sent by the user computer. A host name is text that comes after the @ sign. For example, in account@home.com, the host name is "home.com". If a technician from your ISP helped you set up Internet connection, he/she set the host name as the computer name on your computer (in the Networking screen). When you connect that computer to the Prestige, you must set the same name as the Prestige's system name in SMT menu 1.

```
                    Menu 1 - General Setup

          System Name= zyxel

          Domain Name=

          First System DNS Server= From ISP

            IP Address= N/A

          Second System DNS Server= From ISP

            IP Address= N/A
```

```
                Third System DNS Server= From ISP

                  IP Address= N/A

                Edit Dynamic DNS= No
```

Field Setting:

- System Name: Enter the same name as the compute name on the computer.

---

3. If your ISP checks the User ID

This authentication method is used mostly by ISPs providing RoadRunner services (for example, RR-TAS (Toshiba Authentication Service) or RR-Manager authentication). You must configure the service type, username and password exactly as provided by your ISP in SMT menu 4.

```
                        Menu 4 - Internet Access Setup

                ISP's Name= MyISP

                Encapsulation= Ethernet

                  Service Type= RR-Toshiba

                  My Login= cso@zyxel

                  My Password= ********

                  Retype to Confirm= N/A

                  Login Server= 0.0.0.0

                IP Address Assignment= Dynamic

                  IP Address= N/A
```

```
                    IP Subnet Mask= N/A

                   Gateway IP Address= N/A

                Network Address Translation= SUA Only
```

Field settings:

g. Service Type: Select **RR-TAS** or **RR-Manager** authentication method used by your ISP.
h. Login Server: Enter the IP address of the authentication server if you know it. Otherwise, leave this field to the default to have the Prestige automatically obtain this information.
i. My Login Name: Enter the login user name given to you by your ISP
j. My Password: Enter the password associated with the login name.
k. WAN IP Address Assignment: If the ISP did not assign you a fixed (or static) WAN IP address, select **Dynamic**, otherwise, select **Static**.
l. IP Address, Subnet Mask, Gateway IP Address: If you select **Static** in the **WAN IP Address Assignment** field, enter the IP address, subnet mask and gateway device IP address provided by your ISP.

•

Using Embedded Packet Trace

Embedded Packet Trace

The Prestige packet trace feature records and analyzes packets running on the LAN and WAN interfaces. It is designed for technical users who are interested in the details of the packet flow on the Prestige’ s LAN or WAN interface. It is also a diagnostic tool 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 packet trace result display is as follows:

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 view the trace result:

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

The following details the trace commands in SMT menu 24.8.

Online Trace

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable WAN packet trace: `sys trcp channel enet1 none`
1.2 Enable LAN packet trace: `sys trcp channel enet0 bothway`
1.3 Enable trace logging: `sys trcp sw on` & `sys trcl sw on`
1.4 Display brief online trace results: `sys trcd brief`
or
1.5 Display detailed online trace results: `sys trcd parse`

Example:

```
Prestige> sys trcp channel enet1 none
Prestige> sys trcp channel enet0 bothway
Prestige> sys trcp sw on
Prestige> sys trcl sw on
Prestige> 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
Prestige> 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)
   Identification            = 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)
   Identification           = 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 (64240)
   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)
   Identification            = 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

1.1 Disable LAN packet trace: **sys trcp channel enet0 none**
1.2 Enable WAN packet trace: **sys trcp channel enet1 bothway**
1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
1.4 Display brief online trace results: **sys trcd brief**
or
1.5 Display detailed online trace results: **sys trcd parse**

Example:

```
Prestige> sys trcp channel enet0 none
Prestige> sys trcp channel enet1 bothway
```

```
Prestige> sys trcp sw on
Prestige> sys trcl sw on
Prestige> sys trcd brief
0    12367.680 ENET1-R[0070] UDP 202.132.155.95:520->202.132.155.255:520
1    12370.980 ENET1-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
2    12373.940 ENET1-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
3    12374.930 ENET1-R[0064] TCP 192.31.7.130:80->202.132.155.97:10261
4    12374.940 ENET1-T[0054] TCP 202.132.155.97:10261->192.31.7.130:80
5    12374.940 ENET1-T[0438] TCP 202.132.155.97:10261->192.31.7.130:80
6    12375.320 ENET1-R[0064] TCP 192.31.7.130:80->202.132.155.97:10261
7    12375.360 ENET1-R[0090] UDP 202.132.155.95:520->202.132.155.255:520
Prestige> sys trcd parse
---<0000>--------------------------------------------------------------
LAN Frame: ENET1-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)
    Identification            = 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 (64240)
    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/../...
---<0001>---------------------------------------------------------------
LAN Frame: ENET1-XMIT   Size:  54/  54   Time: 12387.490 sec
Frame Type: TCP 202.132.155.97:10270->192.31.7.130:80


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

  IP Header:
    IP Version              = 4
    Header Length           = 20
    Type of Service         = 0x00 (0)
```

```
    Total Length              = 0x0028 (40)
    Identification             = 0x7A0C (31244)
    Flags                     = 0x02
    Fragment Offset           = 0x00
    Time to Live              = 0x7F (127)
    Protocol                  = 0x06 (TCP)
    Header Checksum           = 0x543C (21564)
    Source IP                 = 0xCA849B61 (202.132.155.97)
    Destination IP            = 0xC01F0782 (192.31.7.130)

  TCP Header:
    Source Port               = 0x281E (10270)
    Destination Port          = 0x0050 (80)
    Sequence Number           = 0x00C18F63 (12685155)
    Ack Number                = 0xD3E95DE9 (3555286505)
    Header Length             = 20
    Flags                     = 0x10 (.A....)
    Window Size               = 0x1DD5 (7637)
    Checksum                  = 0x7A12 (31250)
    Urgent Ptr                = 0x0000 (0)
```

```
  RAW DATA:
  0000: 00 A0 C5 01 23 45 00 A0-C5 92 13 12 08 00 45 00  ....#E........E.
  0010: 00 28 7A 0C 40 00 7F 06-54 3C CA 84 9B 61 C0 1F  .(z.@...T<...a..
  0020: 07 82 28 1E 00 50 00 C1-8F 63 D3 E9 5D E9 50 10  ..(..P...c..].P.
  0030: 1D D5 7A 12 00 00                                ..z...
---<0002>---------------------------------------------------------------
LAN Frame: ENET1-XMIT   Size:  54/  54   Time: 12387.490 sec
Frame Type: TCP 202.132.155.97:10270->192.31.7.130:80
```

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

```
IP Header:
  IP Version              = 4
  Header Length           = 20
  Type of Service         = 0x00 (0)
  Total Length            = 0x0028 (40)
  Identification           = 0x7B0C (31500)
  Flags                   = 0x02
  Fragment Offset         = 0x00
  Time to Live            = 0x7F (127)
  Protocol                = 0x06 (TCP)
  Header Checksum         = 0x533C (21308)
  Source IP               = 0xCA849B61 (202.132.155.97)
  Destination IP          = 0xC01F0782 (192.31.7.130)

TCP Header:
  Source Port             = 0x281E (10270)
  Destination Port        = 0x0050 (80)
  Sequence Number         = 0x00C18F63 (12685155)
  Ack Number              = 0xD3E95DE9 (3555286505)
  Header Length           = 20
  Flags                   = 0x11 (.A...F)
  Window Size             = 0x1DD5 (7637)
  Checksum                = 0x7A11 (31249)
  Urgent Ptr              = 0x0000 (0)

RAW DATA:
0000: 00 A0 C5 01 23 45 00 A0-C5 92 13 12 08 00 45 00  ....#E........E.
0010: 00 28 7B 0C 40 00 7F 06-53 3C CA 84 9B 61 C0 1F  .({.@...S<...a..
0020: 07 82 28 1E 00 50 00 C1-8F 63 D3 E9 5D E9 50 11  ..(..P...c..].P.
0030: 1D D5 7A 11 00 00                                ..z...
Prestige>
```

Offline Trace

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable WAN packet trace: **sys trcp channel enet1 none**
1.2 Enable LAN packet trace: **sys trcp channel enet0 bothway**
1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
1.4 Wait for packets to pass through the Prestige on the LAN
1.5 Disable trace logging: **sys trcp sw off** & **sys trcl sw off**
1.6 Display brief trace results : **sys trcp brief**
1.7 Display specific trace packets: **sys trcp parse <from_index> <to_index>**

Example:

```
Prestige> sys trcp channel enet1 none
Prestige> sys trcp channel enet0 bothway
Prestige> sys trcp sw on
Prestige> sys trcl sw on
Prestige> sys trcp sw off
Prestige> sys trcl sw off
Prestige> sys trcp brief
   0    10855.790 ENET0-T[0141] TCP 192.31.7.130:80->192.168.1.2:1102
   1    10855.800 ENET0-R[0060] TCP 192.168.1.2:1102->192.31.7.130:80
   2    10855.810 ENET0-R[0062] TCP 192.168.1.2:1103->192.31.7.130:80
   3    10855.840 ENET0-R[0062] TCP 192.168.1.2:1104->192.31.7.130:80
   4    10856.020 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1102
   5    10856.030 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1103
   6    10856.040 ENET0-R[0060] TCP 192.168.1.2:1103->192.31.7.130:80
Prestige> sys trcp parse 5 5
```

```
---<0005>----------------------------------------------------------------
LAN Frame: ENET0-XMIT   Size:  58/  58   Time: 10856.030 sec
Frame Type: TCP 192.31.7.130:80->192.168.1.2:1103

  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)
    Identification            = 0x7F02 (32514)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0xED (237)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0x857D (34173)
    Source IP                = 0xC01F0782 (192.31.7.130)
    Destination IP           = 0xC0A80102 (192.168.1.2)


  TCP Header:
    Source Port              = 0x0050 (80)
    Destination Port         = 0x044F (1103)
    Sequence Number          = 0xD91B1826 (3642431526)
    Ack Number               = 0x00AA405F (11157599)
    Header Length            = 24
    Flags                    = 0x12 (.A..S.)
    Window Size              = 0xFAF0 (64240)
    Checksum                 = 0xDCEF (56559)
    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 7F 02 40 00 ED 06-85 7D C0 1F 07 82 C0 A8  .,..@....}......
  0020: 01 02 00 50 04 4F D9 1B-18 26 00 AA 40 5F 60 12  ...P.O...&..@_`.
  0030: FA F0 DC EF 00 00 02 04-05 B4                    ..........
Prestige>
```

2. Trace WAN packet

1.1 Disable LAN packet trace: **sys trcp channel enet0 none**
1.2 Enable WAN packet trace: **sys trcp channel enet1 bothway**
1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
1.4 Wait for packets to pass through the Prestige on the WAN
1.5 Disable trace logging: **sys trcp sw off** & **sys trcl sw off**
1.6 Display brief trace results: **sys trcp brief**
1.7 Display specific trace packets: **sys trcp parse <from_index> <to_index>**

Example:

```
Prestige> sys trcp channel enet0 none
Prestige> sys trcp channel enet1 bothway
Prestige> sys trcl sw on
Prestige> sys trcp sw on
Prestige> sys trcl sw off
Prestige> sys trcp sw off
Prestige> sys trcp brief
   0    12864.800 ENET1-T[0411] TCP 202.132.155.97:10278->204.217.0.2:80
   1    12864.890 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10282
   2    12864.900 ENET1-T[0416] TCP 202.132.155.97:10282->204.217.0.2:80
   3    12865.120 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10278
   4    12865.130 ENET1-T[0411] TCP 202.132.155.97:10278->204.217.0.2:80
   5    12865.220 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10282
Prestige> sys trcp parse 3 4
---<0003>--------------------------------------------------------------
```

```
LAN Frame: ENET1-RECV   Size: 247/  96   Time: 12865.120 sec
Frame Type: TCP 204.217.0.2:80->202.132.155.97:10278

  Ethernet Header:
    Destination MAC Addr     = 00A0C5921312
    Source MAC Addr          = 00A0C5591284
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x00E5 (229)
    Identification            = 0xE93B (59707)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0xF0 (240)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0x6E15 (28181)
    Source IP                = 0xCCD90002 (204.217.0.2)
    Destination IP           = 0xCA849B61 (202.132.155.97)


  TCP Header:
    Source Port              = 0x0050 (80)
    Destination Port         = 0x2826 (10278)
    Sequence Number          = 0x4D713D8A (1299266954)
    Ack Number               = 0x00C8C015 (13156373)
    Header Length            = 20
    Flags                    = 0x18 (.AP...)
    Window Size              = 0x2238 (8760)
    Checksum                 = 0xAB57 (43863)
    Urgent Ptr               = 0x0000 (0)


  TCP Data: (Length=193, Captured=42)
  0000: 48 54 54 50 2F 31 2E 31-20 33 30 34 20 4E 6F 74  HTTP/1.1 304 Not
```

```
  0010: 20 4D 6F 64 69 66 69 65-64 0D 0A 44 61 74 65 3A   Modified..Date:
  0020: 20 57 65 64 2C 20 30 37-20 4A                     Wed, 07 J

  RAW DATA:
  0000: 00 A0 C5 92 13 12 00 A0-C5 59 12 84 08 00 45 00  .........Y....E.
  0010: 00 E5 E9 3B 40 00 F0 06-6E 15 CC D9 00 02 CA 84  ...;@...n.......
  0020: 9B 61 00 50 28 26 4D 71-3D 8A 00 C8 C0 15 50 18  .a.P(&Mq=.....P.
  0030: 22 38 AB 57 00 00 48 54-54 50 2F 31 2E 31 20 33  "8.W..HTTP/1.1 3
  0040: 30 34 20 4E 6F 74 20 4D-6F 64 69 66 69 65 64 0D  04 Not Modified.
  0050: 0A 44 61 74 65 3A 20 57-65 64 2C 20 30 37 20 4A  .Date: Wed, 07 J
---<0004>--------------------------------------------------------------
LAN Frame: ENET1-XMIT   Size: 411/  96   Time: 12865.130 sec
Frame Type: TCP 202.132.155.97:10278->204.217.0.2:80


  Ethernet Header:
    Destination MAC Addr     = 00A0C5591284
    Source MAC Addr          = 00A0C5921312
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x018D (397)
    Identification            = 0xF20C (61964)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0x7F (127)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0xD59C (54684)
    Source IP                = 0xCA849B61 (202.132.155.97)
    Destination IP           = 0xCCD90002 (204.217.0.2)


  TCP Header:
    Source Port              = 0x2826 (10278)
```

```
   Destination Port         = 0x0050 (80)
   Sequence Number          = 0x00C8C015 (13156373)
   Ack Number               = 0x4D713E47 (1299267143)
   Header Length            = 20
   Flags                    = 0x18 (.AP...)
   Window Size              = 0x1E87 (7815)
   Checksum                 = 0x4374 (17268)
   Urgent Ptr               = 0x0000 (0)

 TCP Data: (Length=357, Captured=42)
 0000: 47 45 54 20 2F 70 69 63-74 75 72 65 73 2F 6D 61  GET /pictures/ma
 0010: 67 61 7A 69 6E 65 5F 6C-6F 67 6F 2F 62 65 73 74  gazine_logo/best
 0020: 6F 66 74 69 6D 65 73 2E-67 69                    oftimes.gi

 RAW DATA:
 0000: 00 A0 C5 59 12 84 00 A0-C5 92 13 12 08 00 45 00  ...Y..........E.
 0010: 01 8D F2 0C 40 00 7F 06-D5 9C CA 84 9B 61 CC D9  ....@........a..
 0020: 00 02 28 26 00 50 00 C8-C0 15 4D 71 3E 47 50 18  ..(&.P....Mq>GP.
 0030: 1E 87 43 74 00 00 47 45-54 20 2F 70 69 63 74 75  ..Ct..GET /pictu
 0040: 72 65 73 2F 6D 61 67 61-7A 69 6E 65 5F 6C 6F 67  res/magazine_log
 0050: 6F 2F 62 65 73 74 6F 66-74 69 6D 65 73 2E 67 69  o/bestoftimes.gi
Prestige>
```

Debugging PPPoE Connection

Debugging PPPoE Connection

You can use the packet trace tool on the Prestige to troubleshoot PPPoE Internet connection. Follow the procedure below to perform packet trace for troubleshooting.

1. Remove the Ethernet cable from the LAN port on the Prestige

2. Enter the SMT through the console port
3. Enter SMT Menu 24.8-CI command mode
4. Type the following commands:
   - sys trcp sw on (turn on packet trace)
   - sys errctl 3 (save crash information and set the system to enter the mode after the crash)
   - poe debug 1 (turn on pppoe debug)
   - dev dial 1 (dial to remote node 1)
5. After you have entered the commands, you can send the saved logs in case your Prestige crashes and there's nothing you can do to bring the connection up.
6. If the Prestige crashes and you are able to enter the command mode, enter 'atds' in debug mode to display the logs. Copy the logs and send them to us.
7. If the Prestige does not crash but you still can not dial out to your ISP for Internet connection. Capture the following logs. Copy the logs and send them to us.
   - sys trcp sw off (turn off packet trace)
   - sys log disp i (display system error logs)
   - sys trcp parse (display detailed trace results)

Example- Trace Example on a crashed system

```
ras> sys trcp sw on
ras> sys errctl 3
ras> poe debug 1
ras> dev dial 1
Start dialing for node <GPMI>...
poeNetCmdExe: chann poe0 event x420
poeChannDial: start session, peer<GPMI>
bdcastInit: pch poe0
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
bdcastSendInit: l1.pktTx() failed, pch poe0 ch enet0
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
```

```
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0.........
poeI/C: ver 1 type 1 code x07 sessId x0000 len 274(x0112)
poeCtrlI/C: pkt len 274
poeGetTags()
service-name
service-name telstra
service-name bpa
service-name iprimus
service-name pacificinternet
service-name integrationisp
service-name bpa-dev
service-name bpa-sif
service-name telstrarna
service-name gpmsystems
service-name cmux
service-name launceston-broadband
service-name vivanet
service-name n1234567k00
service-name bigpond
service-name n7061992k
service-name n3068223k
service-name n2155202k
service-name n7061995k
AC-name vet1-exhibition-bsn-1
host-uniq 31303030 len 4
PADO recv'd, chann enet1
procPADO: for poe chann poe0
Chann poe0 sending request
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x19 sess-id 0 len 12(x000C)
Undefined Address : 0xE3F045C4
Undefined Data : 0x56FF54FF
    r0= 0xE3F045C4    r1= 0x0001FFC0    r2= 0x000000E5    r3= 0x56FF54FF
    r4= 0xE3F045C4    r5= 0xE5BDBFEC    r6= 0x0001C468    r7= 0x60000093
    r8= 0x00000000    r9= 0xE3550000     r10=0xE3550000    fp= 0x00000000
```

```
    r12=0x56FF54FF    sp= 0x0001EDBC    lr= 0x00004F64    pc= 0x00013954
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
e5bdbfe0: e2 8f 00 06 e5 d5 20 06 e5 d5 20 0a e5 d5 20 0e ...b...f...j...n
e5bdbff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc000: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc010: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc020: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc030: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc040: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc050: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc060: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc070: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc080: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc090: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
Bootbase Version: V1.06 | 11/05/2004 19:29:47
RAM: Size = 8192 Kbytes
DRAM POST: Testing:  8192K
OK
FLASH: Intel 16M

ZyNOS Version: V3.60(MM.0) | 12/31/2004 13:39:02
Enter Debug Mode
atgo
    (Compressed)
    Version: RAS P2302RLP1, start: bfc58030
    Length: 3DB3EC, Checksum: 9AA9
    Compressed Length: 12AC58, Checksum: DC06

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:A0:C5:CB:A8:16
initialize ch =1, ethernet address: 00:A0:C5:CB:A8:17
VC5402 Init...OK
```

```
Press ENTER to continue...

                Enter Password : XXXX
```

LAN/WAN Packet Trace

You can use the packet trace feature on the Prestige to record and analyze packets transmitting through the LAN and WAN interfaces. It is designed for technical users who are interested in the details of the packet flow on the Prestige’ s LAN or WAN interface. It is also a very helpful diagnostic tool to solve Internet connection problems or if you want to know the details of a packet for configuring a filter rule.

The format of the result is displayed as follows:

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 display the trace results:

1. **Online Trace--display real-time trace results on the screen**
2. **Offline Trace-- save the trace results first and display them later**

The following shows you how to obtain and display the packet trace results in SMT menu 24.8 are as follows.

Online Trace

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable capture the WAN packet trace: **sys trcp channel mpoa00 none**

1.2 Enable capture the LAN packet trace: **sys trcp channel enet0 bothway**

1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**

1.4 Display brief online trace results: **sys trcd brief**

or

1.5 Display detailed online trace results: **sys trcd parse**

Example:

```
ras> sys trcp channel mpoa00 none
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on
ras> sys trcl sw on
ras> 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    11883.2602HW ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  10    11883.2602HW ENET0-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80
ras> 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)
    Identification             = 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               = 0x2004 (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)
  Identification            = 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 (2602HW40)
  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)
   Identification            = 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

1.1 Disable LAN packet trace: **sys trcp channel enet0 none**
1.2 Enable WAN packet trace: **sys trcp channel mpoa00 bothway**
1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
1.4 Display brief online trace results: **sys trcd brief**
or
1.5 Display detailed online trace results: **sys trcd parse**

Example:

```
ras> sys trcp channel enet0 none
ras> sys trcp channel mpoa00 bothway
ras> sys trcp sw on
ras> sys trcl sw on
ras> 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
ras> 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)
  Identification            = 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 (2602HW40)
  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

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable WAN packet trace: `sys trcp channel mpoa00 none`
1.2 Enable LAN packet trace: `sys trcp channel enet0 bothway`
1.3 Enable trace logging: `sys trcp sw on` & **`sys trcl sw on`**
1.4 Wait for packets to pass through the Prestige on the LAN
1.5 Disable trace logging: `sys trcp sw off` & **`sys trcl sw off`**
1.6 Display brief trace results: `sys trcp brief`
1.7 Display specific packet trace results: `sys trcp parse <from_index> <to_index>`

2. Trace WAN packet

1.1 Disable LAN packet trace: `sys trcp channel enet0 none`
1.2 Enable WAN packet trace: `sys trcp channel mpoa00 bothway`
1.3 Enable trace logging: `sys trcp sw on` & **`sys trcl sw on`**
1.4 Wait for packets to pass through the Prestige on the WAN
1.5 Disable trace logging: `sys trcp sw off` & **`sys trcl sw off`**
1.6 Display brief trace results: `sys trcp brief`
1.7 Display specific packet trace results: `sys trcp parse <from_index> <to_index>`

CLI Command List

The most updated CI command list is available in the release notes with every ZyXEL firmware release. Download the latest firmware package (*.zip), from ZyXEL's public WEB site at http://www.zyxel.com/support/download.php. You must unzip the package to get the release note in PDF format.