P-2608HWL Series

Support Notes

Version 3.40

August. 2006

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 the Windows
- Setting up the Prestige router
- Troubleshooting

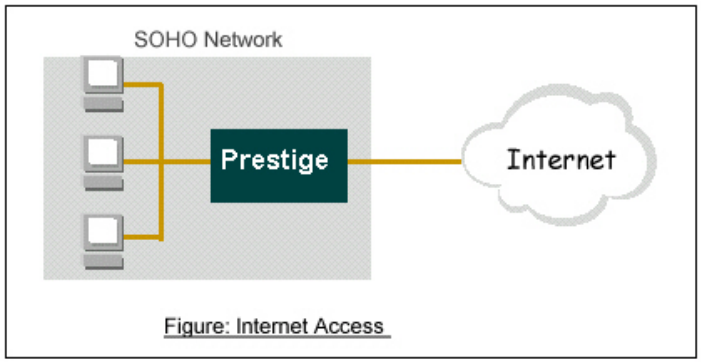


Figure: Internet Access

- Before you begin

The Prestige is shipped with the following factory defaults:

1. IP address = 192.168.1.1, subnet mask = 255.255.255.0 (24 bits)
2. DHCP server enabled with client IP address pool starting from 192.168.1.33
3. Default SMT login 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 the TCP/IP software on each computer before you can use it for Internet access. If you have already installed TCP/IP, skip to the next section; otherwise, follow these steps to install the software:

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

3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

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

Note: Do not assign an arbitrary IP address and subnet mask to your computers. O otherwise, you will not be able to access the Internet.

- Click the **WINS** configuration tab and select **Disable WINS Resolution**.
- Click the **Gateway** tab. Highlight any installed gateways and click the **Remove** button until there are 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 powered on before clicking **Yes**. Repeat the above steps for each 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

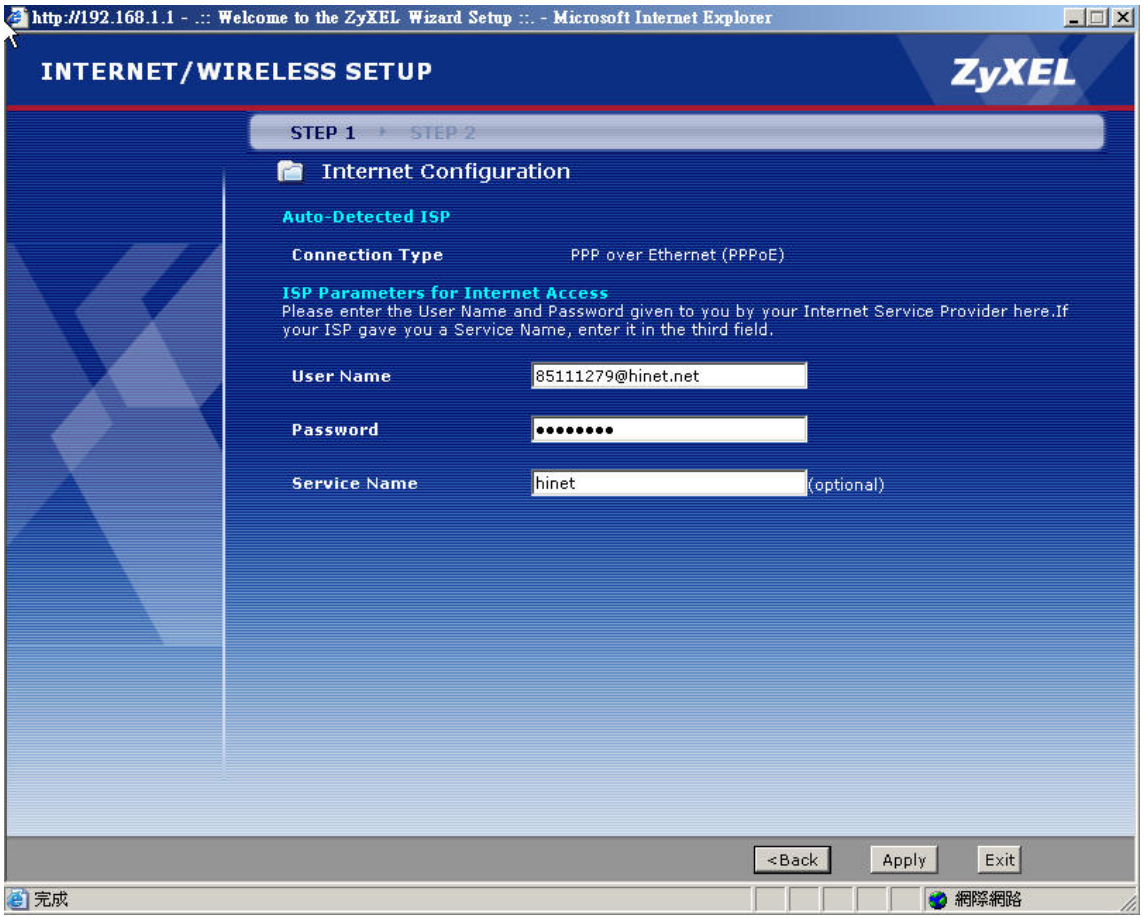
Open your web browser (such as IE) and enter the LAN IP address of the Prestige in the Address field. The default LAN IP address is 192.168.1.1.

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 SETUPscreens 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.



Set up 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-2608 as a DHCP server or DHCP relay.

When the P-2608 is configured as a DHCP server, it assigns IP address to clients on the LAN. When the P-2608 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.

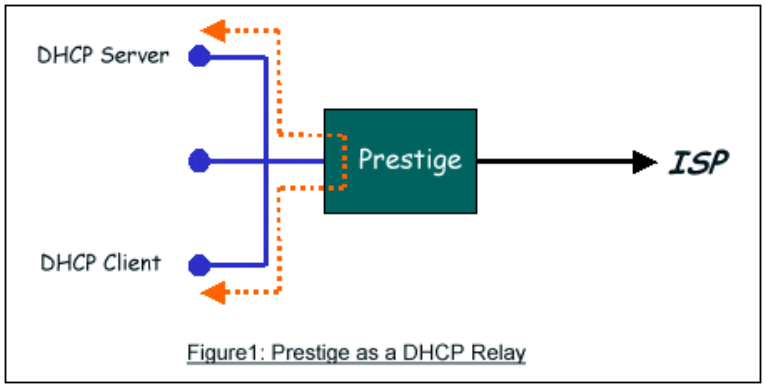


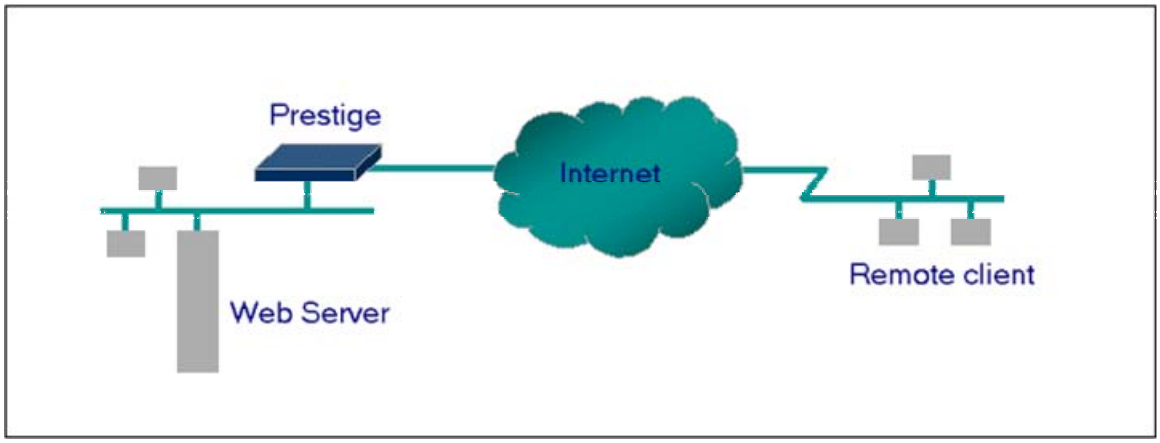
Figure1: Prestige as a DHCP Relay

- Setup the Prestige as a DHCP Relay

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

```
                Menu 3.2 - TCP/IP and DHCP 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= None
  IP Address= N/A                      Version= N/A
Second DNS Server= N/A               Multicast= None
  IP Address= N/A                    IP Policies=
Third DNS Server= N/A                Edit IP Alias= No
  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 P-2608 assessable/visible to the outside world. A server behind the P-2608 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. 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

```
                Menu 15.2 - NAT Server Setup


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

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

- 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

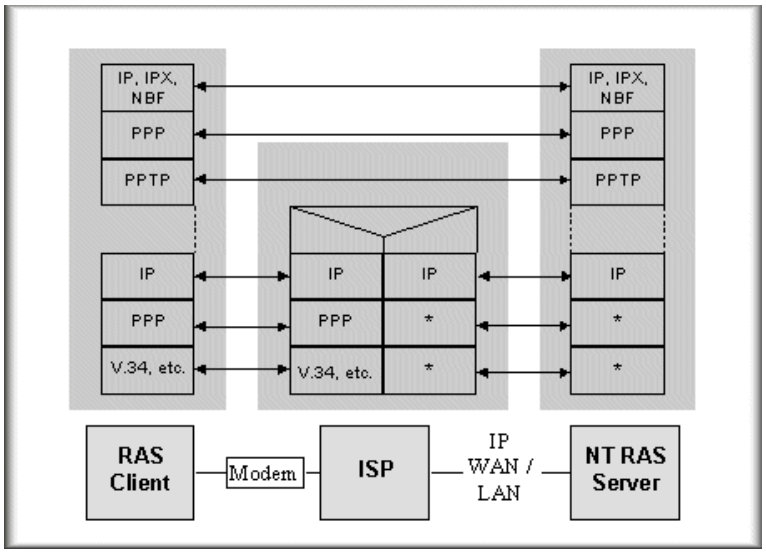
Configure a PPTP server Behind SUA

- 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.



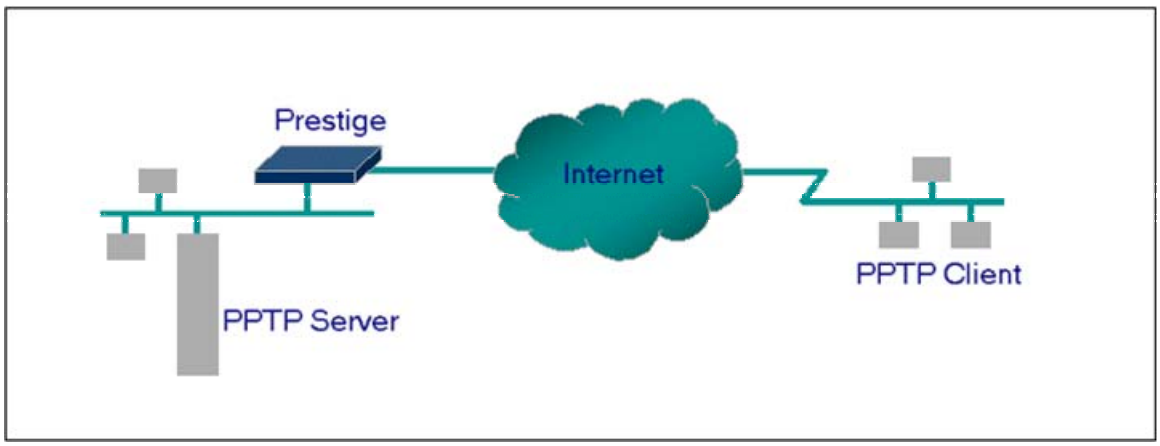
Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

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.

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 the PPTP server (Windows NT server), the 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 or TCP/IP NetBEUI) for the RAS port
  - Set the Prestige as the Internet gateway
- PPTP client setup (Windows 9x)

- 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 secure VPN connection from the PPTP client to the PPTP server, you must first connect the Prestige to the ISP for Internet access.
- Enter the IP address and the port number of the PPTP server to allow public access to the server behind the Prestige. The following shows a configuration example.

```
                Menu 15.2 - NAT Server Setup


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

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

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 which is set to use the SUA feature. 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.

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.

Using NAT / Multi-NAT

- What is Multi-NAT?

NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. Inside and outside networks are networks relative to the Prestige. The network connected behind the Prestige is the "inside network" while the remote network (such as the Internet) is the "outside network". When a packet is received from the inside hosts, NAT maps and changes the source IP address of the received packets to one or more IP addresses known to the outside network. When a packet is received from the outside network, NAT unmaps and changes the outside source IP address back to the local IP address known to the inside network. The Prestige WAN IP address for NAT can be static (fixed) or dynamically assigned by the ISP. In addition, you can also make one or more servers on the inside network visible/accessible to the outside network. If no specified inside server is defined, NAT provides an added layer of security to filter traffic to the Prestige and prevent network probing/port scanning.

With SUA (Single User Account) supports, the Prestige maps the private (local) IP addresses to one global (WAN) IP address. This means you can only have one NAT behind the Prestige. To allow more than one NATs behind the Prestige, RFC 1631, *The IP Network Address Translator (NAT)* is implemented in ZyNOS V3.40 for the Prestige. This feature is also known as Multi-NAT. For more information, refer to RFC 1631.

- How NAT works

Internal Local Addresses (ILA) refer to the local or private IP addresses known to the local network and Inside Global Address (IGA) refers to the public or global IP address known to the outside network. The following figure shows a network example. NAT operates by mapping the ILA to the IGA required for communication with hosts on other networks. That means NAT replaces the original source IP address in the packets with the global IP address. To the outside network, this makes the packets look as if they originate from the Prestige and not from the inside computers. The Prestige keeps a record of the ILA-IGA mappings so packets received from the outside network can be forwarded to the intended computer on the inside network.

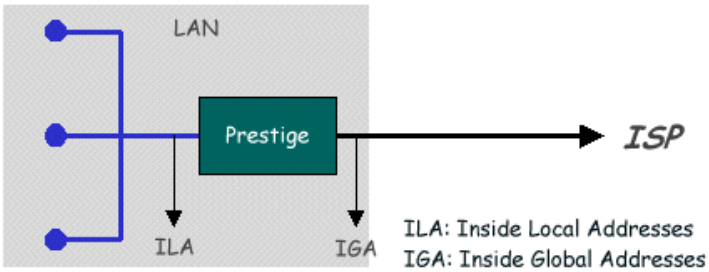


Figure1: Local/Global IP Addresses

1. NAT Mapping Types

The following describes the NAT mapping types.

2. **One to One**

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

3. **Many to One**

In Many-to-One mode, the Prestige maps multiple ILAs to one IGA. This is equivalent to SUA (or PAT, Port Address Translation). ZyXEL's Single User Account (SUA) feature is also supported on routers with the previous ZyNOS version. You can select to use SUA or multi-NAT in ZyXEL routers with ZyNOS V3.40.

4. **Many to Many Overload**

In Many-to-Many Overload mode, the Prestige maps multiple ILAs to a shared IGA.

5. **Many to Many No Overload**

In Many-to-Many No Overload mode, the Prestige maps each ILA to a unique IGA.

- **Server**

In Server mode, the Prestige maps multiple inside servers to one global IP address. This allows you to specify multiple servers for various services behind the Prestige for access from the outside. If you want to map each server to one unique IGA, you must use the One-to-One mode.

The following table summarizes the NAT types.

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

- SUA Versus NAT

ZyXEL's SUA (Single User Account) implementation in the previous ZyNOS versions is similar to having two NAT modes: Many-to-One and Server. With the Full Feature NAT support in ZyNOS v3.40, the Prestige is able to map global IP addresses to local IP addresses. With multiple global IP addresses, multiple severs of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions, you can configure multiple SUA inside servers based on the service ports. However, the SUA inside server settings are limited to one set per remote node. On the Prestige, you can configure multiple NAT entries for each remote node (up to eight). In SMT menu 15.1.1, the default SUA inside server (read-only) Many-to-One mapping setting is pre-configured for users who are already familiar with the SUA feature in the previous ZyNOS versions.

- SMT Menus

1. Applying NAT in the SMT Menus

You can apply NAT in SMT menus 4 and 11.3. The following figure shows how you can set the NAT field in SMT menu 4. From the Main Menu, enter 4 to display SMT menu 4-Internet Access Setup.

```
                Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= PPPoE
Multiplexing= LLC-based
VPI #= 0
VCI #= 33
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= cso@zyxel.net
My Password= ********
Idle Timeout (sec)= 0
IP Address Assignment= Dynamic
  IP Address= N/A
Network Address Translation= Full Feature
  Address Mapping Set= 1

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

The following table describes the options for the Network Address Translation field.

Field	Options	Description
Network Address Translation	**Full Feature**	When you select this option, the SMT will use Address Mapping Set 1 (in SMT menu 15.1 see the following section for more information).
	None	NAT is disabled when you select this option.

	SUA Only	When you select this option, the SMT uses Address Mapping Set 255 (in SMT menu 15.1 see the following section for more information). This is equivalent to the Many-to-One Overload mapping type. The default SUA server setting is set to use IGA **0.0.0.0**. SUA only should work for most network environments. If you want to use other mapping types, select **Full Feature** instead.

Table: Applying NAT in Menu 4 and Menu 11.3

2. Configuring NAT

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

```
                    Menu 15 - NAT Setup

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

3. Address Mapping Sets and NAT Server Sets

Use the Address Mapping Sets menu and submenus to create the mapping table used to replace the source IP address in the packets from inside computers with the global addresses. You must specify a NAT address mapping set to each remote node. Since the P2608HWL Series has eight remote nodes, you need to configure eight NAT address mapping sets. Although there are nine NAT address mapping sets in SMT menu 15.1, you can only configure eight sets (numbered 1 to 8). The ninth set (with the index number of 255) is used for SUA. Thus if you select **Full Feature** NAT in SMT menu 4 or 11.3, NAT address mapping sets 1 to 8 are used. If you select **SUA Only**, then the SMT uses mapping set 255 in menu 15.2.

The NAT Server Set is a list of inside servers (on that LAN) that the Prestige maps to external ports. To apply a NAT Server Set on the Prestige, configure a server rule in the server set menu. Refer to NAT Server Sets for more information on the related configuration menus.

From SMT menu 15, enter 1 to display menu 15.1-Address Mapping Sets as shown.

```
                  Menu 15.1 - Address Mapping Sets

                  1.
                  2.
                  3.
                  4.
                  5.
                  6.
                  7.
                  8.
                255. SUA (read only)
                       Enter Set Number to Edit:
```

The following figure shows the address mapping rules for set 255. NAT address mapping set 255 is used for SUA only and is equivalent to the SUA feature in ZyXEL routers with pre-ZyNOS v3.40 versions. . You cannot changes the fields in this screen.

```
        Menu 15.1.1 - Address Mapping Rules

 Set Name= SUA

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  --------------  --------------  --------------  --------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                         M-1
 2.                                    0.0.0.0                         Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
```

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

The following table explains the read-only fields in this screen.

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

Note that you cannot change the fields in this screen. However, you can change the settings for server set 1 in SMT menu 15.1.1.
Enter 1 in SMT menu 15.1 to display the configuration screen as shown.

```
             Menu 15.1.1 - Address Mapping Rules
 Set Name= ?
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  --------------  --------------  --------------  --------------  ------
 1.
 2.
 3.
 4.
 5.
 6.
 7.
```

```
 8.
 9.
10.
                    Action= Edit          , Select Rule= 0
                    Press ENTER to Confirm or ESC to Cancel:
```

Different from the read-only menu for SUA, you can change the settings in this screen. There are also extra fields in this screen: Action and Select Rule. Note that the [?] in the Set Name field means that this is a required field and you must enter a name for the set. The description of the other fields is as described in the following table. The Type, Local and Global Start/End IPs are configured in Menu 15.1.1 (described later) and the values are displayed here.

Field	Description	Option
Set Name	Enter a name for this set of rules. This is a required field. **Note**: **If this field is left blank, the set will be deleted.**	Rule1
Action	You can specify the action on the rules. The default is **Edit** to modify the rule you select in the **Select Rule** field below. **Insert Before** allows you to insert a new rule before the rule selected. The rule after the selected rule will then be moved down by one rule. **Delete** means to remove the selected rule and then all the rules after the selected one will be advanced one rule. **Save Set** allows you to save the settings of the address mapping set (note that when you choose this action, the **Select Rule** field is not applicable).	Edit Insert Before Delete Save Set
Select Rule	When you choose **Edit**, **Insert Before** or **Save Set** in the **Action** field above, the cursor automatically relocates to this field to allow you to select the number of the rule to which the action is applied.	1

Note: To save the settings of the address mapping set, select Save Set in the Action field. It is recommended that you save the settings every time you make any changes to the address mapping set (this includes deleting a rule). The changes will not take effect until you save the settings. Ordering of the rules is important as rules are applied from top (smallest index number) to bottom.

To change the settings of a rule, select Edit in the Action field and then enter the rule index number in the Select Rule field. The Menu 15.1.1.1-Address Mapping Rule screen displays in which you can edit an individual rule and configure the Type, Local and Global Start/End IPs.

```
Menu 15.1.1.1 -  - Rule 1
Type: One-to-One
Local IP:
  Start= 0.0.0.0
  End  = N/A
Global IP:
  Start= 0.0.0.0
  End  = N/A

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

The following table describes the fields in this screen.

Field		Description	Option/Example
Type		Press [SPACEBAR] to select a mapping type. The various mapping types are discussed in the previous section. The following sections show you some configuration examples.	One-to-One Many-to-One Many-to-Many Overload Many-to-Many No Overload Server
Local IP	Start	This is the starting local IP address (ILA)	0.0.0.0
	End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for **One-to-One** type.	255.255.255.255
Global IP	Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
	End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** types.	200.1.1.64

Note: For all Local and Global IPs, the End IP address must begin after the IP Start address. Thus you cannot have an End IP address that begins before the Start IP address.

- NAT Server Sets

A NAT Server Set is a list of LAN server to external port mappings. This is similar to the SUA menu in the pre-ZyNOS v3.40 SMT). Even though NAT makes your network appears as a single machine to the outside world, you can allow public access to the servers behind NAT. These servers (such as web or FTP servers) will be visible to the external users. A server is identified by a service port number. For example, the Web service runs on port 80 and FTP on port 21.

The following figure shows a network example where there is a web server (192.168.1.36) using port 80 and an FTP server (192.168.1.33) using port 21 in the local network behind NAT.

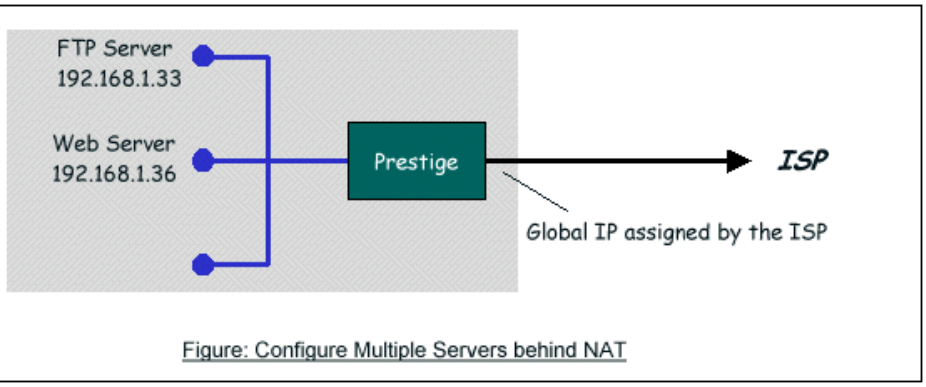


Figure: Configure Multiple Servers behind NAT

Note that you can have more than one service running on the same server. This means that a server can provide both FTP and mail services while another dedicated server provides on the web service.

The procedure below shows you how to configure an inside server behind NAT.

Step 1. From the main menu, enter 15 to go to SMT **Menu 15-NAT Setup**.
Step 2. Enter 2 to go to **Menu 15.2.1-NAT Server Setup**.
Step 3. Enter a service port number in the **Port No.** field and the IP address of the server in the **IP Address** field.
Step 4. Press [SPACEBAR] at the 'Press ENTER to confirm...' prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

```
                Menu 15.2 - NAT Server Setup (Used for SUA Only)

                Rule Start Port No. End Port No. IP Address
               -------------------------------------------------
```

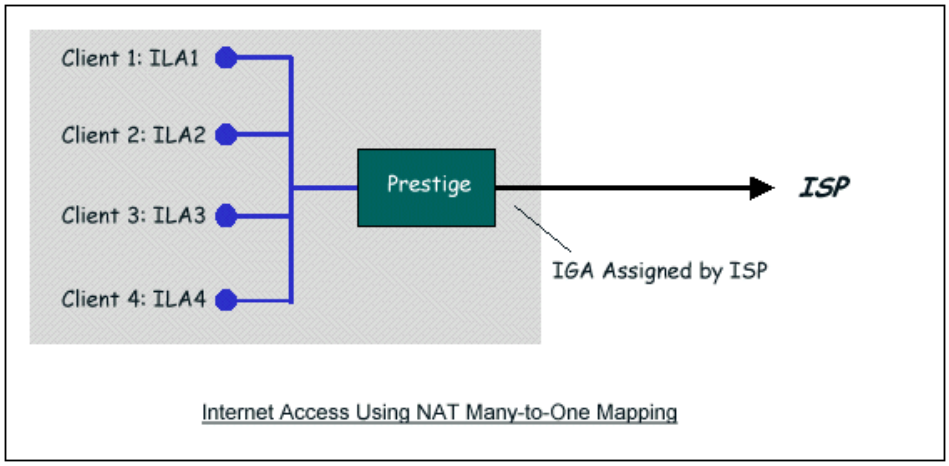
```
                1.      Default       Default       0.0.0.0
                2.        21            21          192.168.1.33
                3.        80            80          192.168.1.36
                4.         0             0          0.0.0.0
                5.         0             0          0.0.0.0
                6.         0             0          0.0.0.0
                7.         0             0          0.0.0.0
                8.         0             0          0.0.0.0
                9.         0             0          0.0.0.0
                10.        0             0          0.0.0.0

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

The most commonly used port numbers are shown in the following table. Refer RFC 1700 for a complete list of service port numbers.

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

1.Internet Access Only

If you do not have a server on the LAN or if you do not wish to allow public access to any inside servers, configure the Prestige for Internet access only. In this case, one rule is needed to map all ILAs to the one IGA assigned by the ISP. The following figure shows a network example.



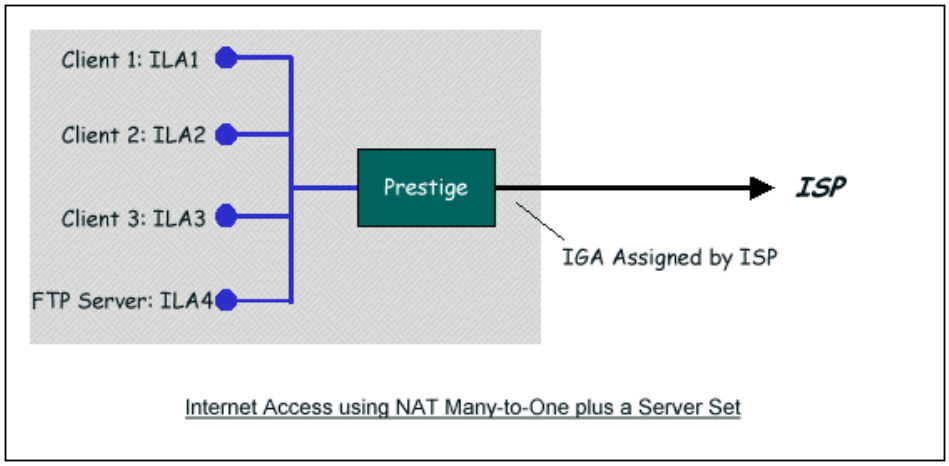
Internet Access Using NAT Many-to-One Mapping

```
        Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= PPPoE
Multiplexing= LLC-based
VPI #= 0
VCI #= 33
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= cso@zyxel
My Password= ********
Idle Timeout (sec)= 0
IP Address Assignment= Dynamic
  IP Address= N/A
Network Address Translation= SUA Only
  Address Mapping Set= 1

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

To configure the Prestige for Internet access only, select **SUA Only** in the **NAT** field in SMT menu 4. This uses the **Many-to-One** mapping discussed earlier. The pre-configured rule (read-only) for SUA is enough to allow this application scenario.

---

2. Internet Access with an Internal Server



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

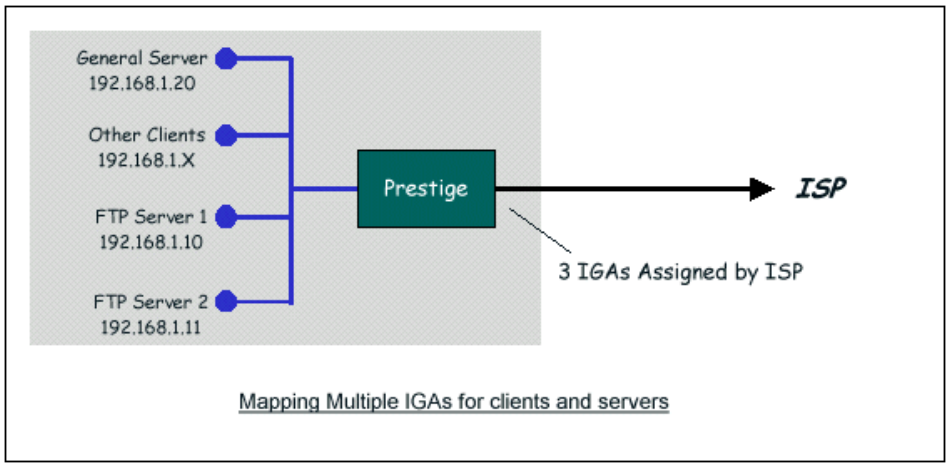
In this case, again select **SUA Only** in the **NAT** field in SMT menus 4 or 11.3. Then go to SMT menu 15.2-NAT Server Setup (Used for SUA Only) to specify the IP address of the Internet server behind NAT as shown in the configuration screen below.

```
Menu 15.2 - NAT Server Setup (Used for SUA Only)

Rule Start Port No. End Port No. IP Address
-------------------------------------------------
 1.     Default      Default      0.0.0.0
 2.       21           21         192.168.1.33
 3.        0            0         0.0.0.0
 4.        0            0         0.0.0.0
 5.        0            0         0.0.0.0
 6.        0            0         0.0.0.0
 7.        0            0         0.0.0.0
```

```
                8.      0       0       0.0.0.0
                9.      0       0       0.0.0.0
                10.     0       0       0.0.0.0

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

---

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



Mapping Multiple IGAs for clients and servers

In this example, we are given 3 IGAs (IGA1, IGA2 and IGA3) by the ISP. Two FTP and one web/mail servers are on the local network. In this case, we configure the following NAT rules to map to the three IGAs.

5. Rule 1 (One-to-One type) maps the FTP Server 1 with ILA1 (192.168.1.10) to IGA1.
6. Rule 2 (One-to-One type) maps the FTP Server 2 with ILA2 (192.168.1.11) to IGA2.
7. Rule 3 (Many-to-One type) maps the other clients to IGA3.
8. Rule 4 (Server type) maps the web and mail server with ILA3 (192.168.1.20) to IGA3. The **Server** rule type allows you to specify more then one inside servers behind NAT on the LAN.

Step 1:

For this example, you have to configure Address Mapping Set 1 in **Menu 15.1-Address Mapping Sets**. Thus you must select **Full Feature** in the **NAT** field in menu 4 or menu 11.3 and set the Prestige to use IGA3 as its WAN IP address.

```
                Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= PPPoE
Multiplexing= LLC-based
VPI #= 0
VCI #= 33
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= cso@zyxel
My Password= ********
Idle Timeout (sec)= 0
IP Address Assignment= Static
  IP Address=IGA 3
Network Address Translation= Full Feature
  Address Mapping Set= 1

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

Step 2:

Go to menu 15.1 and enter 1 (not 255 for SUA this time) to begin configuring this NAT address mapping set. Enter a **Set Name**, select **Edit** in the **Action** field and then enter 1 in the **Select Rule** field. Press [ENTER] to confirm. The following figure shows the four rules for this network example.

For Rule 1: Select **One-to-One** in the **Type** field to map FTP Server 1 with ILA1 (192.168.1.10) to IGA1.

```
                Menu 15.1.1.1 -  - Rule 1
```

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

For Rule 2: Select **One-to-One** in the **Type** field to map FTP Server 2 with ILA2 (192.168.1.11) to IGA2.

```
Menu 15.1.1.2 -  - Rule 2
Type: One-to-One
Local IP:
  Start= 192.168.1.11
  End  = N/A
Global IP:
  Start= [Enter IGA2]
  End  = N/A
Press ENTER to Confirm or ESC to Cancel:
```

For Rule 3: Select **Many-to-One** in the **Type** field to map other LAN clients to IGA3.

```
Menu 15.1.1.3 -  - Rule 3
Type: Many-to-One
Local IP:
  Start= 0.0.0.0
  End  = 255.255.255.255
Global IP:
```

```
                  Start= [Enter IGA3]
                  End  = N/A

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

For Rule 4: Select **Server** in the **Type** field to map the web and mail server with ILA3 (192.168.1.20) to IGA3.

```
                Menu 15.1.1.4 -  - Rule 4
                Type: Server
                Local IP:
                  Start= N/A
                  End  = N/A
                Global IP:
                  Start= [Enter IGA3]
                  End  = N/A

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

After you have configured the mapping rules, menu 15.1.1 should look as follows.

```
                Menu 15.1.1 - Address Mapping Rules
 Set Name= Example3
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  192.168.1.10                      [IGA1]                            1-1
 2.  192.168.1.11                      [IGA2]                            1-1
 3.  0.0.0.0           255.255.255.255 [IGA3]                            M-1
 4.                                    [IGA3]                         Server
 5.
 6.
```

```
 7.
 8.
 9.
10.
                        Press ESC or RETURN to Exit:
```

Step 3:

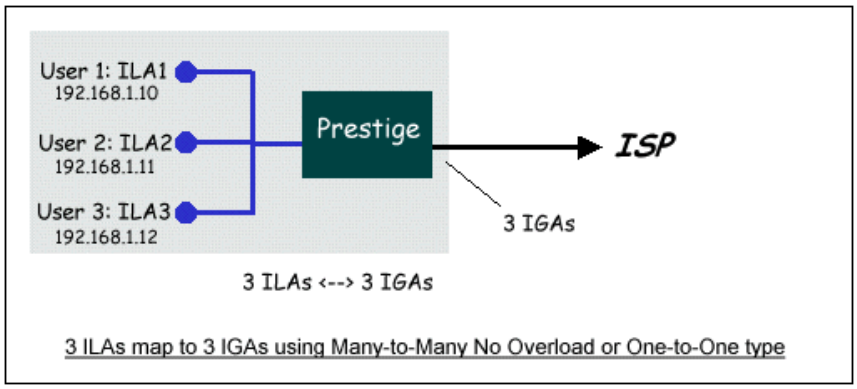
To route web and mail traffic to the inside web/mail server on the LAN, configure **Menu 15.2 - NAT Server Setup** (do not configure Set 1 which is used for SUA).

```
                Menu 15.2 - NAT Server Setup

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

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

---

4. NAT Unfriendly Applications

Some application servers (such as mIRC server) do not allow multiple logins from the same IP address. When you enable NAT on the Prestige, LAN clients behind NAT cannot use these NAT unfriendly applications over the Internet. To allow these applications to work through the Prestige, use Many-to-Many No Overload or One-to-One NAT mapping types to allow each user log into the server using a unique global IP address. The following figure shows a network example.



The following screen shows how to configure a **Many-to-Many No Overload** mapping type for the network example.

```
Menu 15.1.1.1 -  - Rule 1
Type: Many-to-Many No Overload
Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12
Global IP:
  Start= [Enter IGA1]
  End  = [Enter IGA3]

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

The following screens show how to configure a **One-to-One** mapping rule for each IGA.

```
Menu 15.1.1.1 -  - Rule 1

Type: One-to-One
Local IP:
  Start= 192.168.1.10
  End  = N/A
Global IP:
  Start= [Enter IGA1]
  End  = N/A

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

```
Menu 15.1.1.2 -  - Rule 2
Type: One-to-One
Local IP:
  Start= 192.168.1.11
  End  = N/A
Global IP:
  Start= [Enter IGA2]
  End  = N/A

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

```
Menu 15.1.1.3 -  - Rule 3
Type: One-to-One
Local IP:
  Start= 192.168.1.12
  End  = N/A
Global IP:
```

```
                Start= [Enter IGA3]
                End  = N/A

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

You can configure different NAT mapping rules on the Prestige.

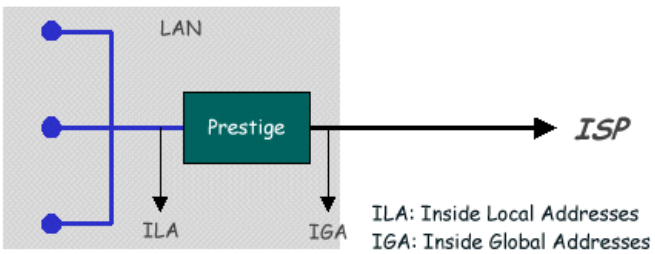


Figure1: Local/Global IP Addresses

The following lists the NAT mapping types on the Prestige.

- SUA
- One to One
- Many to One
- Many to Many overload
- Many One to One
- Server

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2

Many-to-Many No Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server (SUA)	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

Introduction to Filter & Filter Examples

How filters work on ZyXEL devices?

- **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). 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.

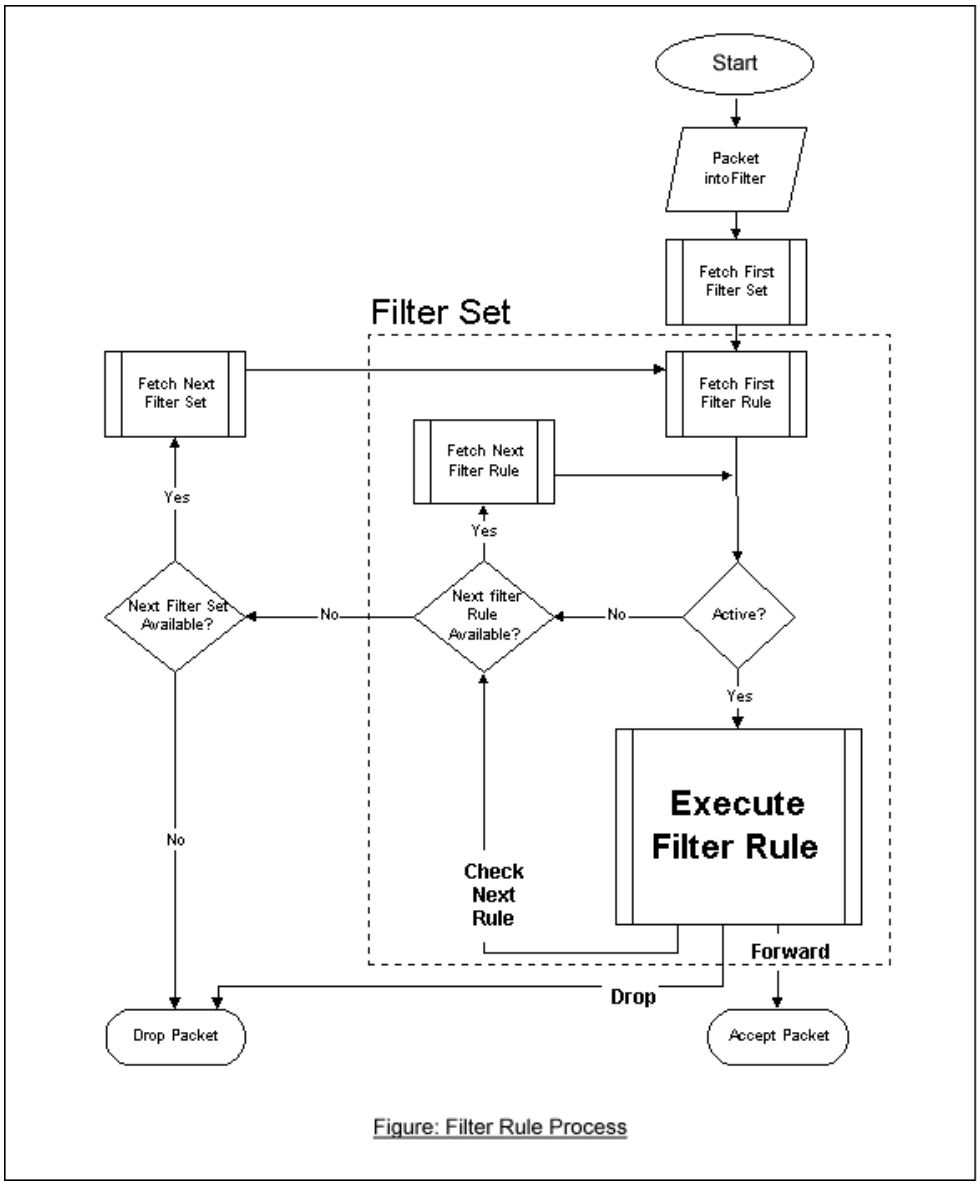


Figure: Filter Rule Process

- **Filter Types and SUA**

You can configure two filter rule categories: device and protocol. 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.

The following figure 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.

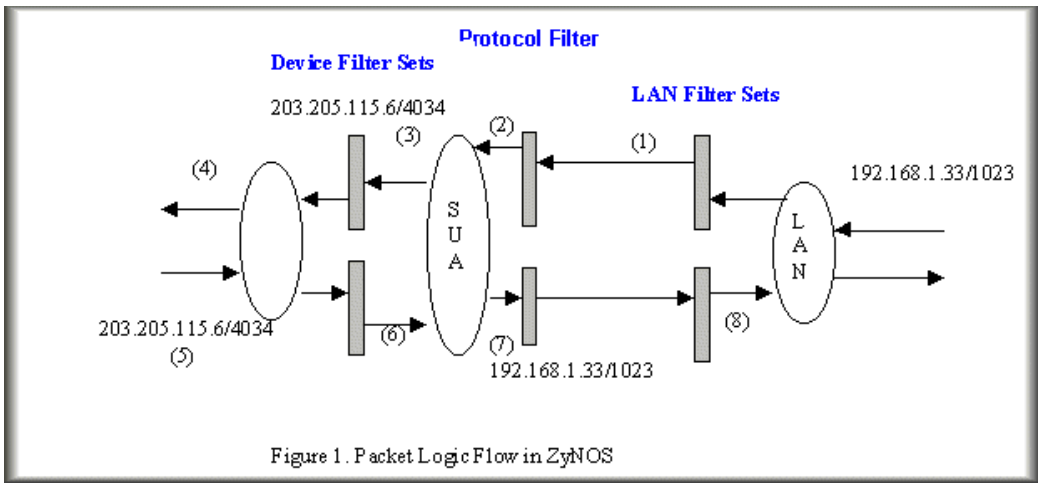


Figure 1. Packet Logic Flow in ZyNOS

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 or 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= PPPoE                Edit IP/Bridge= No

Multiplexing= LLC-based             Edit ATM Options= No

Service Name=                       Edit Advance Options= No

Incoming:                           Telco Option:

  Rem Login= cso@zyxel.net            Allocated Budget(min)= 0

  Rem Password= ********              Period(hr)= 0

Outgoing:                             Schedule Sets=

  My Login= cso@zyxel.net             Nailed-Up Connection= No

  My Password= ********             Session Options:

  Authen= CHAP/PAP                    Edit Filter Sets= Yes

                                      Idle Timeout(sec)= 0

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

Menu 11.5:

```
                    Menu 11.5 - Remote Node Filter


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

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 (protocol & port number)
2. The source IP address

Generally, the outbound packets for 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 Menu 21. For example, set 1
- Create three filter rules in menus 21.1.1, 21.1.2, and 21.1.3
  - Rule 1- block HTTP packets, TCP (06) protocol type with port number 80
  - Rule 2- block DNS packets, TCP (06) protocol type with port number 53
  - Rule 3- block 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. Configure 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 remote node setup.

A filter to block a specific client

Configuration

1. Create a filter set in 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. Configure a 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 LAN computer in this field
IP Mask.....Enter the IP subnet mask bits in this field. Since you can block only one computer, enter 255.255.255.255.
Action Matched.....Select 'Drop' to discard all packets from this computer.
Action Not Matched.....Select 'Forward' to allow 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 client 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)
```

Configuration

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 rule 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. The Prestige will 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', then the packet is considered a match.

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

- Action Not Matched=
  Enter the action you want if the masked packet does not match the 'Value'. In this case, we will forward it. If you want to configure more rules, select 'Check Next Rule' to start configuring another rule. However, note that the 'Filter Type' must also be of the same type (in this example, 'Generic Filter Rule'). You must configure 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 in Menu 3.1 General Ethernet Setup. Note that you can only the Generic Filter in the 'Device Filter' field, but not in the 'Protocol Filter' field, which only allows you to apply TCPIP and IPX filters.

```
Menu 3.1 - General Ethernet Setup
   Input Filter Sets:
     protocol filters=
       device filters= 1
   Output Filter Sets:
     protocol filters=
       device filters=
```

A filter for blocking the NetBIOS packets

- Introduction

The NETBIOS protocol allows the sharing of a Windows computer in a workgroup. For security reasons, the Prestige blocks NetBIOS connection to an outside host by default. To enable the NetBIOS service, remove the filter sets applied in 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 rule 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 remote node setup.

Configure the second filter set 'NetBIOS_LAN' by selecting Filter Set number 2.

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

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

```
                IP Mask= 0.0.0.0
                Port #= 53
                Port # Comp= Equal
        Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 137
                Port # Comp= Equal
TCP Estab= No
More= No            Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

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

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 to block packets from LAN

```
            Menu 3.1 - General Ethernet Setup

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

Using the 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.
- In SMT menu 1, select **Yes** in the **Configure Dynamic DNS** field and press [ENTER]. Menu 1.1 displays.

```
                    Menu 1 - General Setup

          System Name= P2608HWL-D1
          Location=
          Contact Person's Name=
          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= Yes

                Route IP= Yes
                Bridge= No



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

```
                    Menu 1.1 - Configure Dynamic DNS

  Service Provider= WWW.DynDNS.ORG
  Active= Yes
  DDNSType= DynamicDNS
  Host 1= [the local server's host name]
  Host 2= [the local server's host name]
  Host 3= [the local server's host name]
  Username=
  Password= ********
  Enable Wildcard Option= No
  Enable Off Line Option= N/A
  IP Address Update Policy:
    DDNS Server Auto Detect IP Address= No
    Use Specified IP Address= No
    Use IP Address= N/A
                Press ENTER to Confirm or ESC to Cancel:
```

Field Settings for DDNS:

Option	Description
Service Provider	Enter the DDNS server in this field. Currently, the Prestige supports

	WWW.DYNDNS.ORG.
Active	Select **Yes**.
Host	Enter the hostname given by the DDNS service provider. For example, zyxel.com.tw.
EMAIL	Enter the email address you use to register for the account with a DDNS service provider.
User	Enter the user name for the DDNS service account.
Password	Enter the password for the DDNS service account.
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 the management information between network devices (such as routers and switches). By using SNMP, network administrators can easily manage network devices and detect and solve network problems. SNMP is a member of the TCP/IP protocol suite and it uses 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 the 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 setting the variable flags. For example, to reset a node, a counter variable called 'time to reset' could be set to a value which causes the node to reset after the time has 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). The MIB is made up of several parts, including the Standard MIB, specified as part of SNMP, and Enterprise Specific MIB, which are defined by different manufacturer for hardware specific management.

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

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

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 IP routing table) in managed devices.

9. Traps

The managed devices asynchronously report events to NMSs through traps.

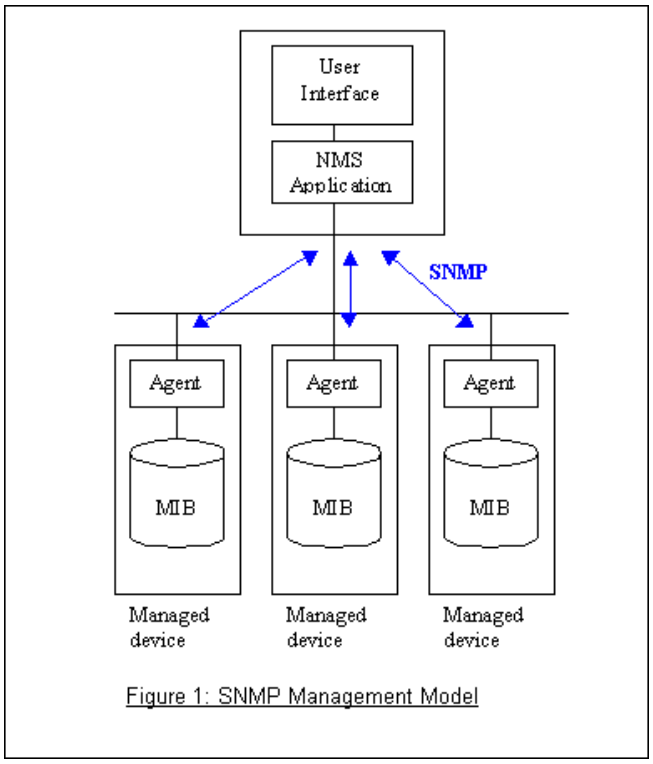


Figure 1: SNMP Management Model

2. SNMPv1 Operations

SNMP itself is a simple request/response protocol. 4 SNMPv1 operations are defined as described 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 the NMS wants to retrieve all entries in a table from an agent, it initiates a Get operation followed by a series of GetNext operations.
- **Set**
  Allows the NMS to set object variable values 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 for the operation. The following figure shows the SNMPv1 message format.

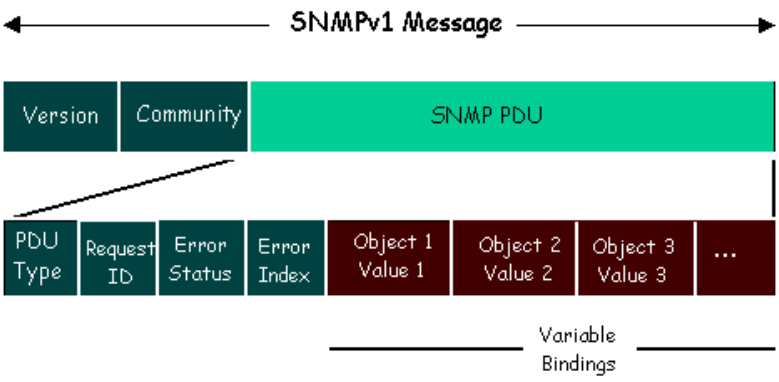


Figure 2: SNMPv1 Message Format

The SNMP PDU contains the following fields:

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

System has to reboot due to unrecoverable errors. Traps with the error codes will be sent.

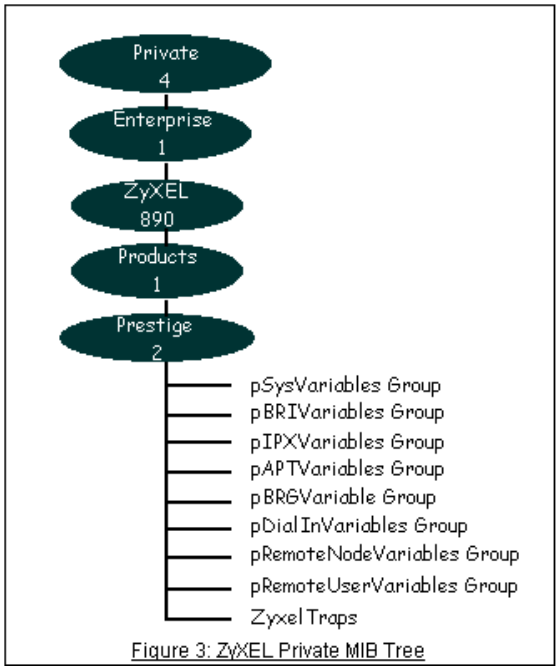
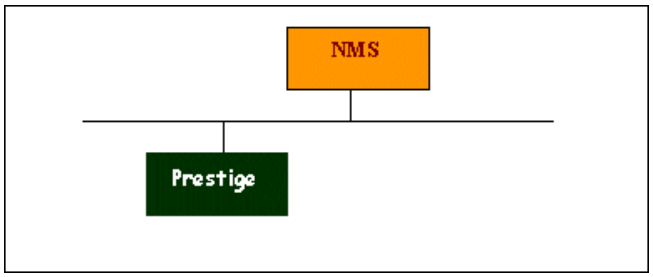


Figure 3: ZyXEL Private MIB Tree

4. Configure the Prestige for SNMP



The SNMP related settings in Prestige are configured in SMT Menu 22 - SNMP Configuration. The configuration procedure is described next.

```
                Menu 22 - SNMP Configuration
SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 192.168.1.33
```

```
                Trap:
                  Community= public
                  Destination= 192.168.1.33

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

Field Settings for SNMP Configuration

Option	Descriptions
Get Community	Enter the Get Community. This Get Community must be the same 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the Set Community. This Set Community must be the same '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 SNMP messages coming from this IP address. **If 0.0.0.0 is entered, 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 to which you wish to send the traps. **If 0.0.0.0 is entered, the Prestige will not send traps to any NMS manager.**

Using syslog

4. **Prestige Setup**

```
Menu 24.3.2 - System Maintenance - UNIX Syslog and Accounting
              UNIX Syslog:
              Active= Yes
              Syslog IP Address= 192.168.1.33
              Log Facility= Local 1
```

Configuration:

1. Active: Press [SPACE] and select Yes to activate syslog logging.
2. Syslog IP Address: Enter the IP address of the UNIX server to which you wish to send the logs.
3. Log Facility. Press [SPACE] to 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 service. The default setting is NOT enabled.

2. Add the following line at the end of the /etc/syslog.conf file.

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

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

3. Restart syslogd.

- **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 indicates the Remote Call ID)
C01 Incoming Call xxxx (indicates connected speed) xxxxx (means Remote Call ID)
L02 Tunnel Connected(L2TP)
C02 OutCall Connected xxxx (indicates the connected speed) xxxxx (indicates 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 send 48 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 activated in the filter rule setting. The message consists of the packet header and the filter rule 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

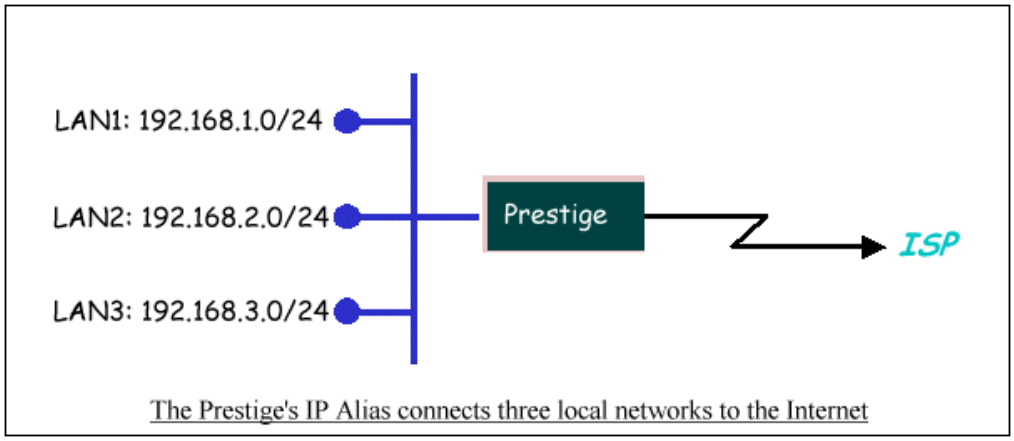
Example:

```
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 another 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.

- IP Alias Setup

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

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

                DHCP Setup
                  DHCP= Server
                  Client IP Pool Starting Address= 192.168.1.33
                  Size of Client IP Pool= 32
                  Primary DNS Server= 0.0.0.0
                  Secondary DNS Server= 0.0.0.0
                  Remote DHCP Server= N/A
                TCP/IP Setup:
                  IP Address= 192.168.1.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= None
                    Version= N/A
                  Multicast= None
                  IP Policies=
                  Edit IP Alias= Yes

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

Field Settings for TCP/IP and DHCP Setup:

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 for IP Alias Setup:

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 third route entry on the enif0:1 interface.

Using Call Scheduling

1. What is Call Scheduling ?

Call scheduling is a mechanism that allows the Prestige to establish a connection to the remote node based on the pre-defined schedule. This feature is similar to the pre-set record time setting in a video recorder. On the Prestige, you can apply up to four schedule sets in SMT Menu 11 – Remote Note Setup. Use SMT Menu 26 – Schedule Setup to configure the schedule settings. For scheduled actions, you can set the Prestige to **Force On**, **Force Down**, **Enable Dial On-Demand** or **Disable Dial-On-Demand** for the connection to the remote node.

- SMT Menu for Call Scheduling

1. Configure schedule set settings in menu 26:

```
                Copyright (c) 1994 - 2006 ZyXEL Communications Corp.

                        P-2608HWL- D1 Main Menu

 Getting Started                    Advanced Management
   1. General Setup                   21. Filter and Firewall Setup
   2. WAN Backup Setup                22. SNMP Configuration
   3. LAN Setup                       23. System Security
   4. Internet Access Setup           24. System Maintenance
                                      25. IP Routing Policy Setup
 Advanced Applications                26. Schedule Setup
   11. Remote Node Setup              27. VPN/IPSec Setup
   12. Static Routing Setup

   15. NAT Setup                      99. Exit

                     Enter Menu Selection Number:
```

2. Select a schedule set number and enter a descriptive name.

```
                Menu 26 - Schedule Setup

            Schedule                  Schedule
            Set # Name                Set # Name
```

```
------ ----------------    ------ ----------------
1 ZyXEL                    7 ________________
2 ________________         8 ________________
3 ________________         9 ________________
4 ________________        10 ________________
5 ________________        11 ________________
6 ________________        12 ________________

     Enter Schedule Set Number to Configure= 1

     Edit Name= ZyXEL

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

3. Specify the number of the schedule set to configure and configure SMT Menu 26.1-Schedule Set Setup as shown.

```
          Menu 26.1 Schedule Set Setup

Active= Yes
Start Date(yyyy-mm-dd)= 2004 - 01 - 01
How Often= Once
Once:
  Date(yyyy-mm-dd)= 2004 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time(hh:mm)= 12 : 00
Duration(hh:mm)= 16 : 00
Action= Enable Dial-on-demand
```

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

Field Settings for Schedule Set Setup:

Start Date	Start date of this schedule rule. If you set the time in the **Once** field, the **Weekdays** setting is not applicable. For example, if **Start Date** is 2004/10/02 (which is a Monday), you don't have to specify the **Monday** field under **Weekdays**.
How Often	If you select **Once**, all fields under **Weekdays** are **N/A**.
Forced On	If you select **Force On** in the **Action** field, the connection to the remote node is always up during the specific time. This is equivalent to disabling the idle timeout feature.
Forced Down	If you select **Forced Down** in the **Action** field, the connection to the remote node is terminated during the specified time.
Enable Dial-On-Demand	If you select **Enable Dial-On-Demand** in the **Action** field, the Prestige establishes a connection to the remote node during the specified time when there is outbound traffic to the WAN.
Disable Dial-On-Demand	If you select **Disable Dial-On-Demand** in the **Action** field, the Prestige disallows connection to the remote node. If there is already connection to the remote node, the Prestige terminates the connection and disables trigger dial up.
Start Time/ Duration	Specify the Start Time and Duration of this schedule.

- Apply the schedule to the Remote node

You can apply more than one schedule sets to a remote node in menu 11.1. However, the schedule sets are applied in the order they are entered in the Schedules field. In addition, if you have conflicting schedule settings in the schedule sets applies, the higher priority schedule set replaces the setting of the lower priority schedule set(s). The following figure shows an example where schedule sets 1, 2, 3 and 4 are applied to the remote node. In this case, schedule set 1 has the highest priority and its settings replace the settings of schedule set 2. Likewise, schedule 2 settings applied will over-write settings applied in schedule 3 and so on.

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

```
Rem Node Name= MyISP                Route= IP
Active= Yes

Encapsulation= PPPoE                Edit IP= No
Service Type= Standard              Telco Option:
Service Name=                         Allocated Budget(min)= 0
Outgoing:                             Period(hr)= 0
  My Login= cso@zyxel                 Schedules= 1,2,3,4
  My Password= ********               Nailed-Up Connection= No
  Retype to Confirm= ********
  Authen= CHAP/PAP
                                    Session Options:
                                      Edit Filter Sets= No
                                      Idle Timeout(sec)= 100

                                    Edit Traffic Redirect= No

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

- System Date and Time Setup

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.

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


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

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

Current Date: 2004 - 01 - 01
New Date (yyyy-mm-dd): 2004 - 01 - 01

Time Zone= GMT+0800

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

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

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. Through IGMP, IP hosts report multicast group membership information to any immediate-neighbor multicast routers which decide if a multicast packet needs to be forwarded.

During start up, the Prestige queries all directly connected networks to gather multicast 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 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= None
  IP Address= N/A                     Version= N/A
Second DNS Server= From ISP         Multicast= IGMP-v2
  IP Address= N/A                   IP Policies=
Third DNS Server= From ISP          Edit IP Alias= No
  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 Options:                         Bridge Options:
  IP Address Assignment = Dynamic     Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= N/A
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= None
    Version= RIP-2B
  Multicast= IGMP-v2
```

```
                IP Policies=


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

Field Settings for Multicast Setup

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

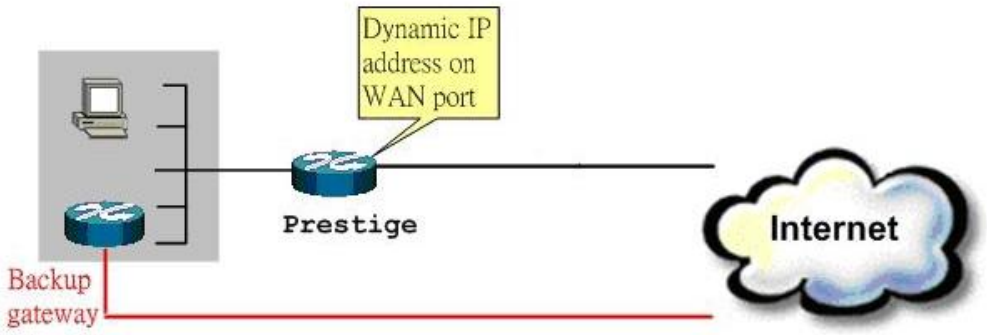
Using traffic redirect

- 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 makes your backup gateway 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 deploy backup gateway?

Set up the backup gateway device in the LAN network behind the Prestige as shown in the example figure below.



Traffic Redirect on LAN port

- 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.

```
Menu 2 - Wan Backup Setup
```

```
                        Menu 2 - Wan Backup Setup

                Check Mechanism = DSL Link
                Check WAN IP Address1 = 0.0.0.0
                Check WAN IP Address2 = 0.0.0.0
                Check WAN IP Address3 = 0.0.0.0
                  KeepAlive Fail Tolerance = 5
                  Recovery Interval(sec) = 60
                  ICMP Timeout(sec) = 0
                Traffic Redirect = Yes
```

Field Settings for WAN Backup Setup:

Label	Description
Backup Type	Select the method that the Prestige uses to check the DSL connection. Select **DSL Link** to have the Prestige check if the connection to the DSLAM is up. Select **ICMP** to have the Prestige periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	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). **If you select ICMP in the** Backup Type **field, you must configure at least one IP address here**. When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
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).
Recovery	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically

Label	Description
Interval	checks to determine whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.
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.
Traffic Redirect	
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down. **If you activate traffic redirect, you must configure at least one** Check WAN IP Address**.**
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Using Universal Plug n Play (UPnP)

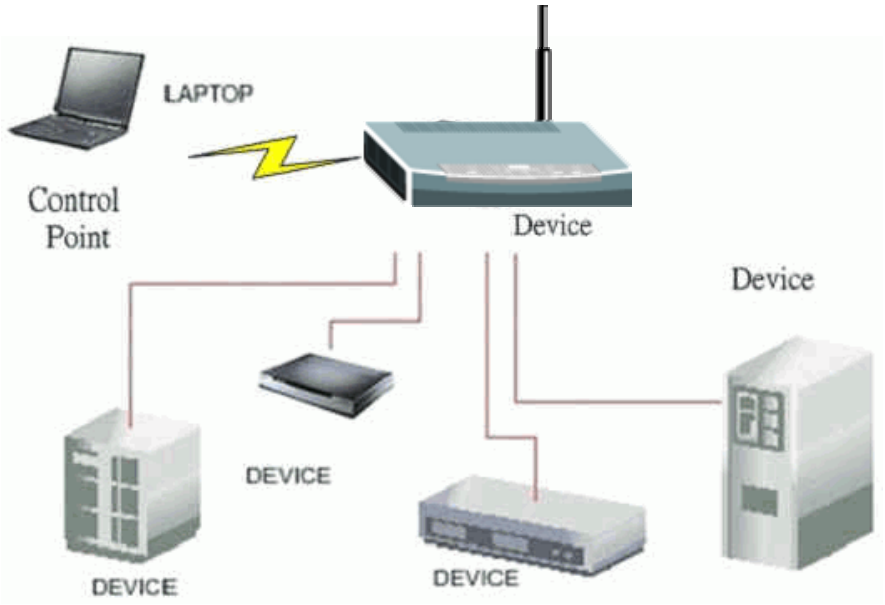
- **1. What is UPnP**

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 can automatically solve 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 respond with their URLs and device descriptions.



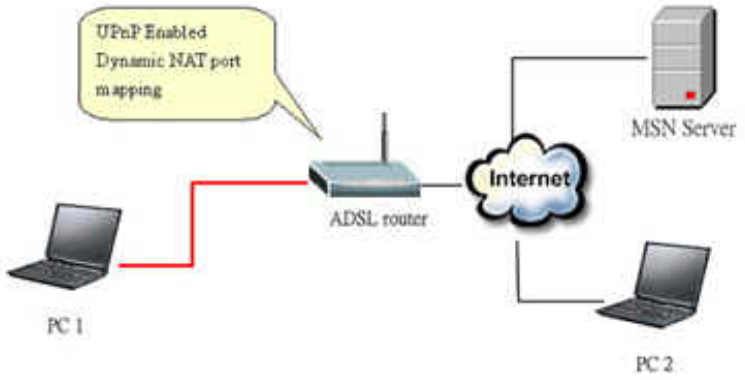
UPnP Operations

- Addressing: UPnPv1 devices MAY support IPv4, IPv6, or both. For IPv4, each device should be set to act 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. Control point can also discover services provided by devices.
- Description: Control points can obtain detailed service information from the devices 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 messages.
- 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 the 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 application 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).



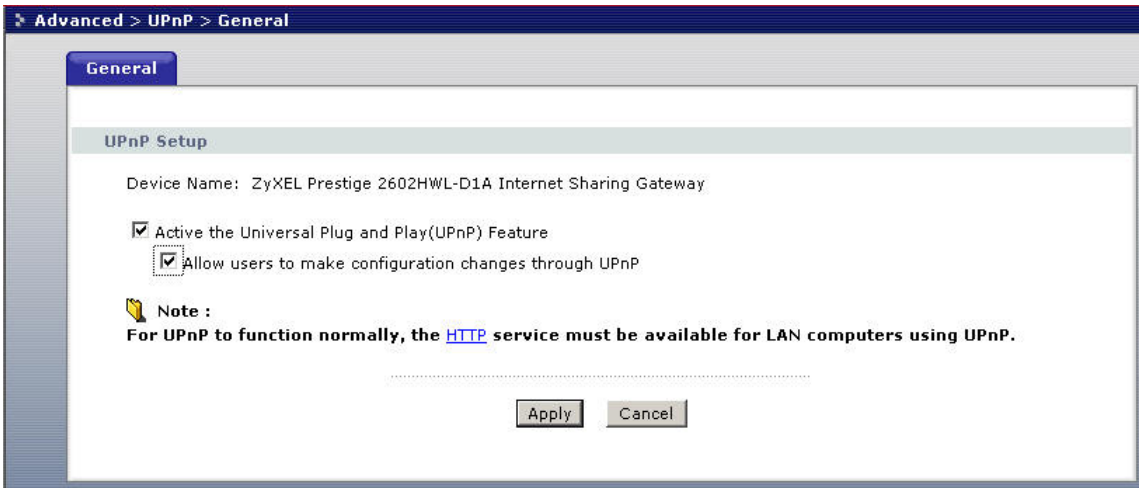
Device: Prestige Router
Service: NAT function provided on the Prestige
Control Point: PC1

1. Enable the UPnP function in a ZyXEL device

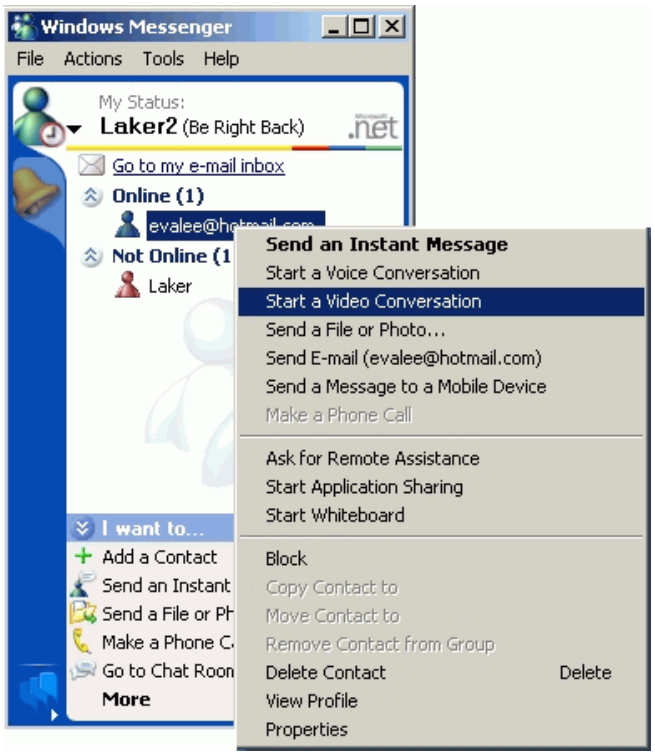
To enable UPnP on a ZyXEL device, log into the web management interface and click **Advanced->UPnP**. Then select the **Active UPnP feature** and **Allow users to make configuration changes through UPnP** check boxes.

Selecting the **Active UPnP feature** check box enables the UPnP function on this device.

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.

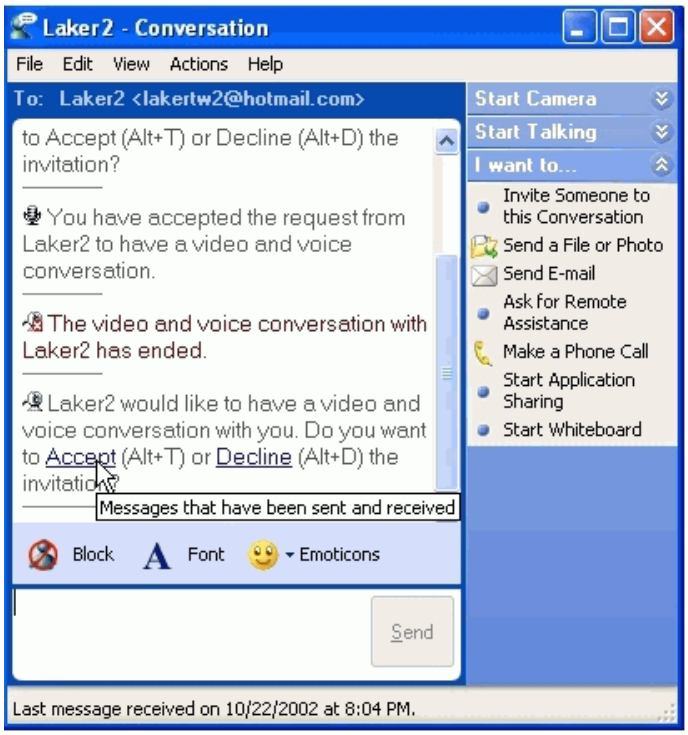


2. After the dynamic port mapping is created and that your computer has obtained an IP address from the Prestige, you can launch the MSN application and connect to the MSN server.

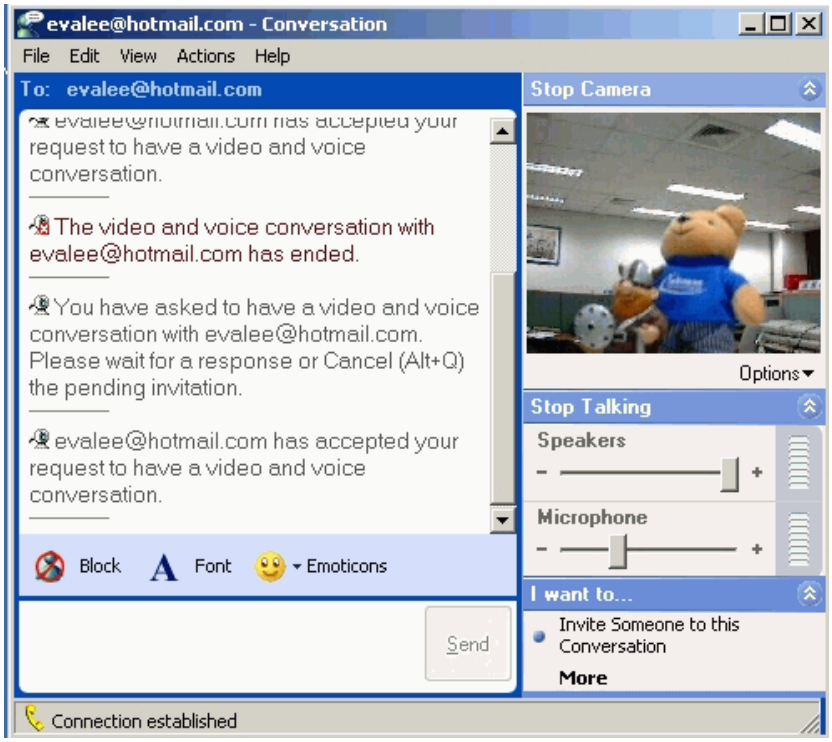


3. After a successful sign-in, you can start a video conversation with another MSN user.

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



5. Finally, you and the remote MSN user can start the video conversation.

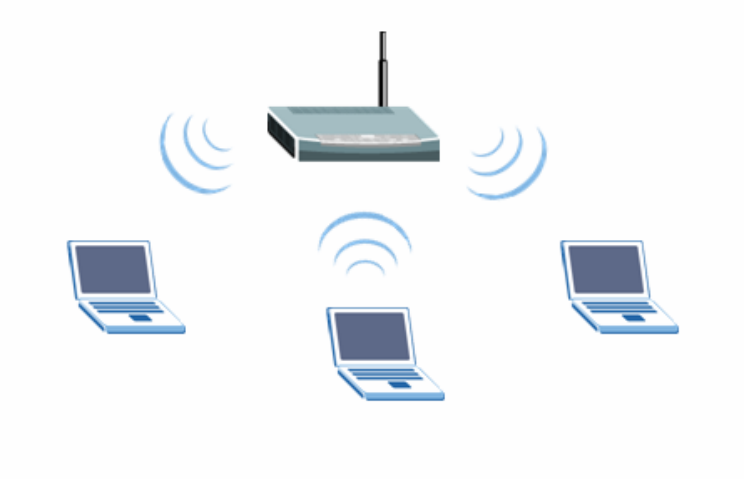


Wireless Application Notes

Infrastructure mode

What is Infrastructure mode?

Infrastructure mode, sometimes referred to as the Access Point mode, is an operating mode you can select on an IEEE 802.11b/Wi-Fi client. In infrastructure mode, the wireless client can associate with an IEEE 802.11b/Wi-Fi Access Point in order to communicate with other wireless clients that also connect to the same AP in infrastructure mode.



WLAN Configuration on the Prestige Using the SMT.

Following steps below to configure Infrastructure mode on your Prestige using the SMT.

1. From the SMT main menu, enter 3 to display Menu 3 – LAN Setup.

2. Enter 5 to display Menu 3.5 – Wireless LAN Setup.

```
                Menu 3.5- Wireless LAN Setup

        ESSID= ZyXEL
        Hide ESSID= No
        Channel ID= CH06 2437MHz
        RTS Threshold= 2432
        Frag. Threshold= 2432
        WEP= Disable
          Default Key= N/A
          Key1= N/A
          Key2= N/A
          Key3= N/A
          Key4= N/A
        Edit MAC Address Filter= No
```

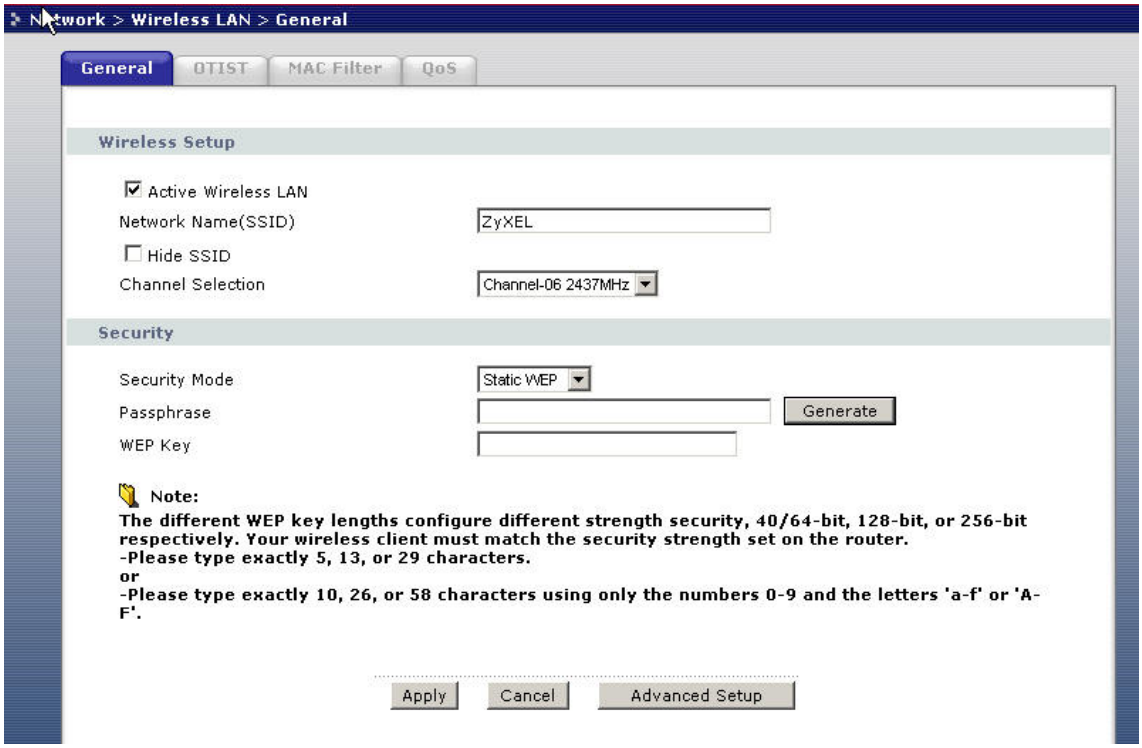
```
                Press ENTER to Confirm or ESC to Cancel:
```

3. Set the ESSID, Channel ID, WEP, Default Key and Keys as you desire.

WLAN Configuration on the Prestige Using the Web Configurator

Following steps below to configure Infrastructure mode on your Prestige using the web configurator.

1. From the web configurator main menu, click **Network >Wireless LAN** to display the **Wireless Setup** screen.



3. Configure the wireless setting on the Prestige and select the **Active wireless LAN** check box.

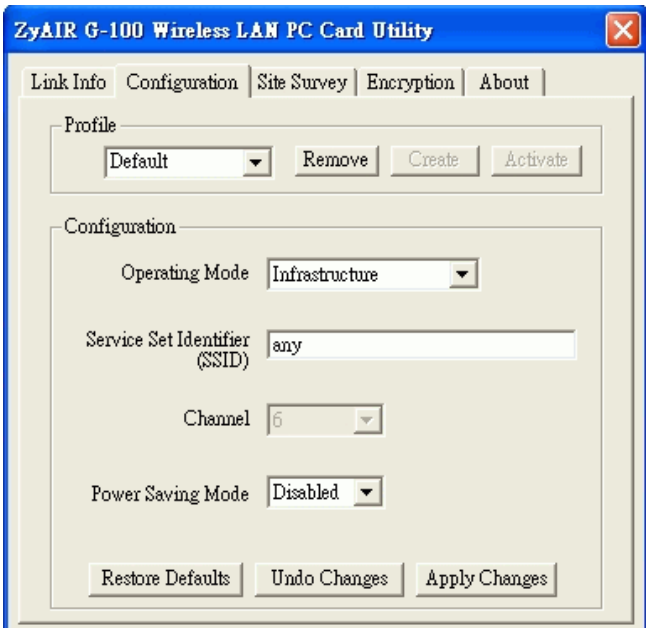
4. Click **Apply** to make the changes take effect.

- *Configuring the Wireless Client*

Follow the steps below to configure a wireless client (such as ZyXEL’ s B-100, B-200 or B-300 wireless client adaptor) to connect to the Prestige.

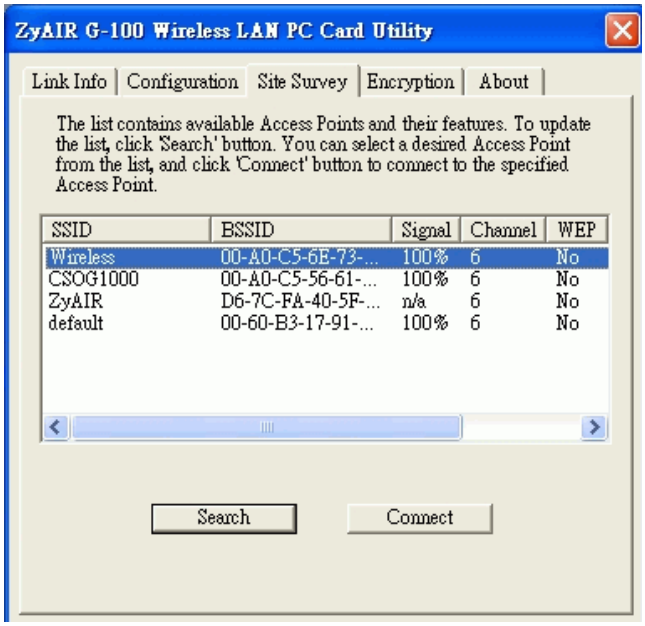
1. Double-click on the ZyXEL wireless utility icon in your windows task bar to display the utility screen.

2. Click the **Configuration** tab.

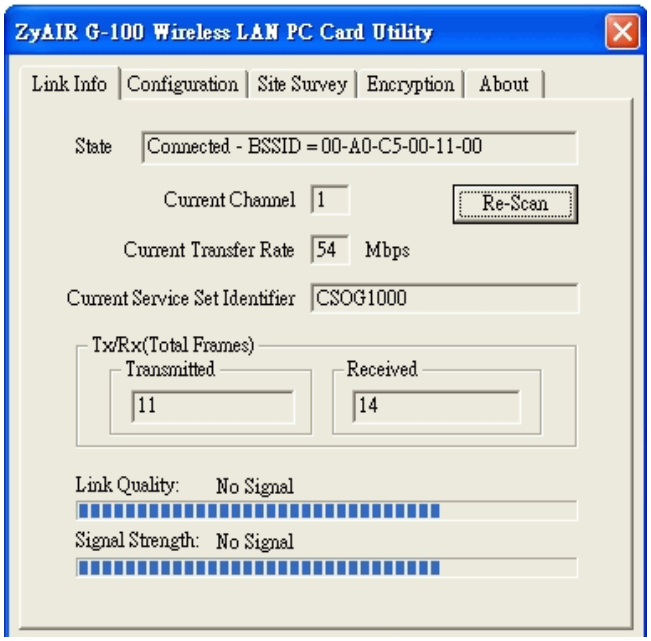


3. Select **Infrastructure** in the **Operation Mode** drop-down list menu. Enter the SSID or leave it to **any** if you wish to connect to any AP. Click **Apply Changes** to save the settings.

4. Click the **Site Survey** tab, and press **Search** to detect and display all the available APs in the list.



5. Double-click on the AP you want to associate with.

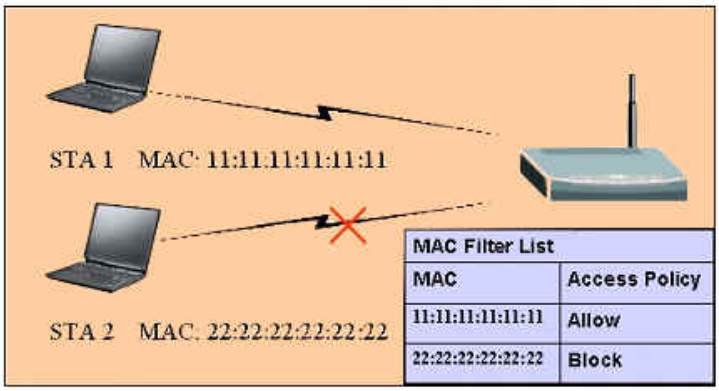


6. After the client has connected to the selected AP, the connected AP's information (such as the channel, current connection speed, SSID, link quality, and signal strength) displays in the Link Info screen. This also indicates that you have successfully connected to the selected AP in infrastructure mode.

Wireless MAC address filtering

MAC Filter Overview

You can use the MAC Filter feature to restrict unauthorized wireless clients from accessing to the AP. With this feature, ZyXEL APs are able to check the MAC address of a wireless client before allowing it to connect to the network. This provides an additional layer of control in that wireless clients with the allowed MAC addresses can connect to the network All you need to do is to specify the list of allowed or blocked MAC addresses on the AP.



---

2. ZyXEL MAC Filter Implementation

ZyXEL's MAC Filter implementation allows you to define a list to allowed or blocked wireless station MAC addresses. You can configure up to 12 entries in the list. Two filter actions are available: Allow Association and Deny Association. Select the Allow Association action to allow only the wireless clients with the MAC addresses listed to access the network via the AP. Wireless clients with unlisted MAC addresses are denied access. Similarly, select the Deny Association action to prevent wireless clients with the listed MAC addresses from accessing the network while wireless clients with unlisted MAC address are allowed access.

---

3. MAC Filter Configuration Using the SMT

Configure the MAC Filter on the Prestige in SMT Menu 3.5.1 - WLAN MAC Address Filter Configuration. Before you configure the MAC filter, you must first obtain the MAC address of the wireless client (use the **ipconfig /all** DOS command on the wireless client).

The following figure shows the SMT configuration menu for MAC filter.

Enter the MAC addresses of the wireless clients in the fields provided and select the filter action to allow or block access.

```
                Menu 3.5.1 - WLAN MAC Address Filter

                        Active= Yes
                        Filter Action= Allowed Association
-------------------------------------------------------------------------------
  1=   11:11:11:11:11:11   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
  2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
  3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
  4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
  5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
  6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
  7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
  8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
  9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
 10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
 11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
 12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
-------------------------------------------------------------------------------
                    Enter here to CONFIRM or ESC to CANCEL:
```

Field Settings For MAC Filter Setup

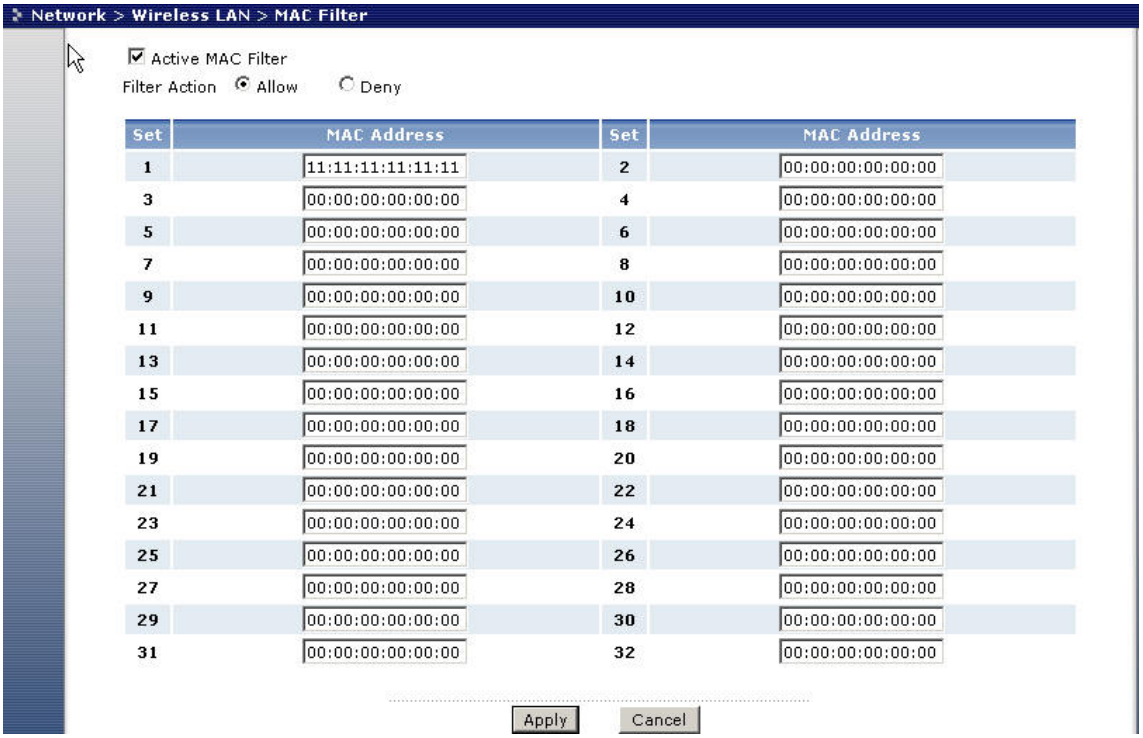
Option	Descriptions
Filter Action	Allow or block association from MAC addresses contained in this list. If **Allow Association** is selected in this field, hosts with MAC addresses configured in this list will be allowed to

	associate with the AP. If **Deny Association** is selected in this field, hosts with MAC addresses configured in this list will be blocked.
MAC Address	Enter the MAC addresses of a wireless client you want to control access.

MAC Filter Configuration Using the Web Configurator

Follow the steps below to configure MAC Filter in the web configurator.

1. Log into the web configurator on the AP by entering the LAN management IP address in a web browser. The default LAN management IP address is **192.168.1.1** and the default login password is **1234**.
2. Click **Network** > **Wireless LAN**.
3. Click the **MAC Filter** link and select **Active MAC Filter** to enable MAC Filter.
4. Specify the **Filter Action** to allow or deny association from wireless clients with the listed MAC addresses.
5. Enter the MAC addresses of the wireless clients you want to allow or block associations from.
6. Click **Apply** to save the settings.



WEP (Wired Equivalent Privacy)

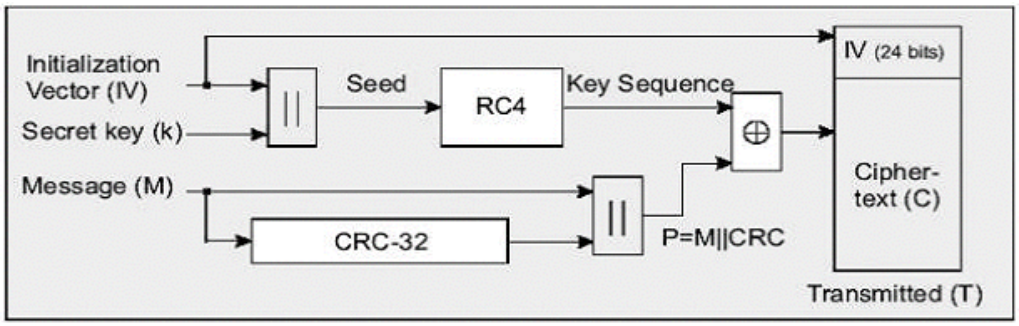
Introduction

The IEEE 802.11 standard set out the communication protocols for wireless LANs.

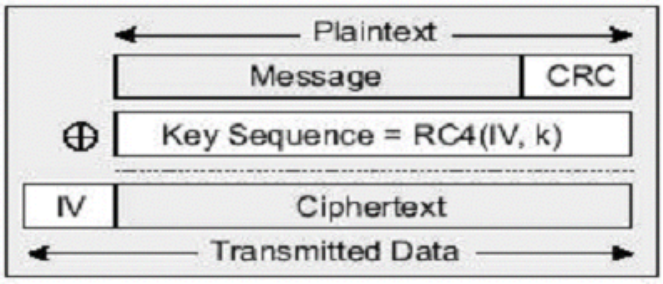
Wired Equivalent Privacy (WEP) data encryption protects wireless communication from eavesdropping, because wireless transmission is easier to intercept than transmission over wired networks, and a wireless network is a shared medium on which data can be intercepted by anyone on the same network.

WEP relies on a secret key that is shared between a wireless client (for example,. a laptop with a wireless Ethernet card) and an access point (such as a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that the packages are not modified during transition. The standard does not discuss how the shared key is established. In practice, most implementations use a single key that is shared between all wireless clients and access points.

WEP uses the Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG) key encryption algorithm. The same key is used to encrypt and decrypt the data.



WEP provides a simple defense against attacks. To avoid encrypting two cipher texts with the same key stream, an Initialization Vector (IV) is used to augment the shared WEP key (secret key) and produce a different RC4 key for each packet. There are two WEP key (secret key) types: 64-bit and 128-bit. They are sometimes referred to as 40-bit and 104-bit. The reason for the different term used is that the 40/104-bit WEP key is concatenated with the initialization vector (24 bits) resulting in a total key size of 64/128 bits.



Setting up the Access Point

On most access points and wireless clients, you can configure up to four WEP keys. Specify the four WEP keys and select one default key to use for data encryption. The following lists the different key types and keys you can configure.

- 64-bit WEP key (secret key) with 5 characters
- 64-bit WEP key (secret key) with 10 hexadecimal digits
- 128-bit WEP key (secret key) with 13 characters
- 128-bit WEP key (secret key) with 26 hexadecimal digits

You can configure the WEP keys on a ZyXEL AP using the SMT or the web configurator.

- WEP Key Configuration on the Access Point Using the SMT

Set up the WEP keys in SMT Menu 3.5 – Wireless LAN Setup. You can configure up to four WEP keys on the Prestige and specify one default key to use for data encryption.
For example,

```
                    3.5- Wireless LAN Setup
                ESSID= Wireless
                Hide ESSID= No
```

```
Channel ID= CH07 2442MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= 64-bit WEP
  Default Key= 3
  Key1= 2e3f4
  Key2= 5y7js
  Key3= 24fg7
  Key4= 98jui
Edit MAC Address Filter= No
```

Field settings for WEP Key Setup

Precede a hexadecimal WEP key with a '**0x**',

WEP Key type	Example
64-bit WEP with 5 characters	Key1= 2e3f4 Key2= 5y7js Key3= 24fg7 Key4= 98jui
64-bit WEP with 10 hexadecimal digits ('0-9', 'A-F')	Key1= **0x**123456789A Key2= **0x**23456789AB Key3= **0x**3456789ABC Key4= **0x**456789ABCD
128-bit WEP with 13 characters	Key1= 2e3f4w345ytre Key2= 5y7jse8r4i038 Key3= 24fg70okx3fr7 Key4= 98jui2wss35u4
128-bit WEP with 26 hexadecimal digits ('0-9', 'A-F')	Key1= **0x**1122334455667788 99AABBCDEF Key2= **0x**2233445566778899AABBCCDDEE Key3= **0x**3344556677889900AABBCCDDFF Key4= **0x**44556677889900AABBCCDDEEFF

Select one of the WEP key as the default key to use for data encryption. .
The remote wireless client will use the corresponding key to decrypt the data received.

For example, if an access point use Key 3 to encrypt data, then a wireless client will use Key 3 to decrypt the received data.
So, the wireless client and the access point use the same key in Key 3.
Although the access point uses Key 3 as the default key, the station can use the other key as its default key to encrypt data. As shown in the following.

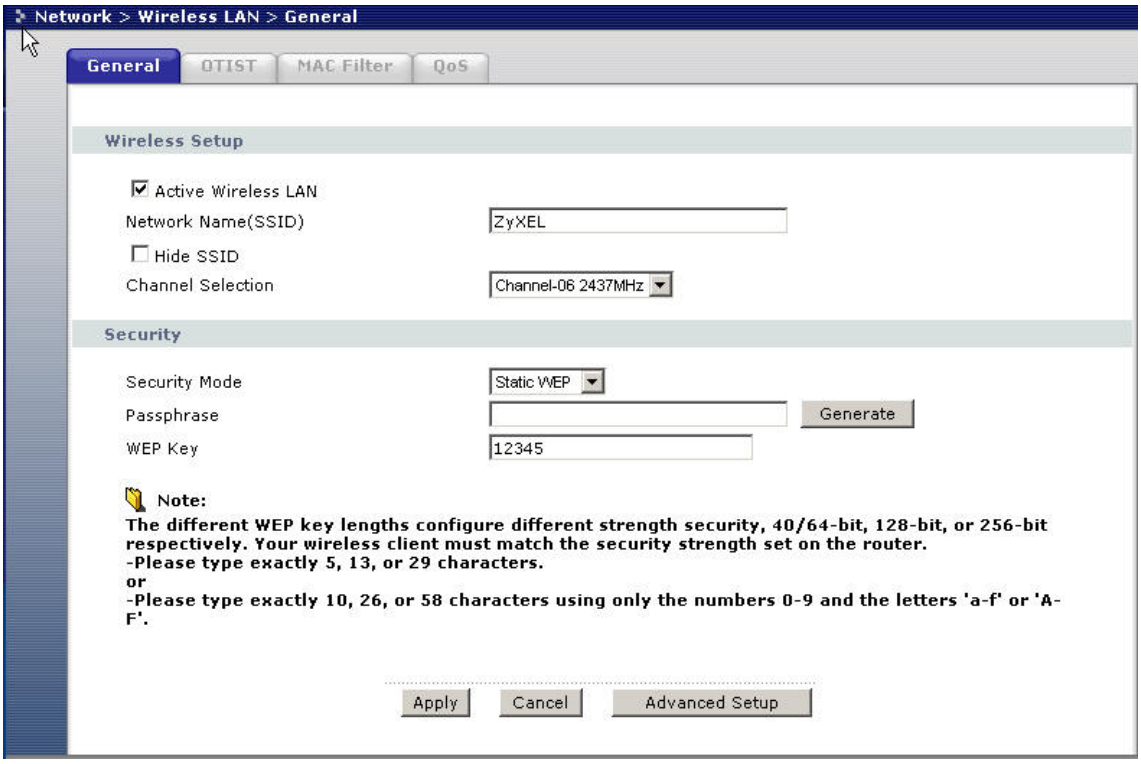
Access Point (encrypt data by Key 3) --------> Station (decrypt data by Key 3)

Access Point (decrypt data by Key 2) <-------- Station (encrypt data by Key 2)

In this case, the access point encrypts data with Key 3 and transmits the encrypted data to the wireless client. The wireless client decrypts the received data using its Key 3.

Similarly when the wireless client encrypts data with Key 2 and sends the encrypted data to the access point, the access point will use its Key 2 to decrypt the received data.

- WEP Key Configuration on the Access Point Using the Web Configurator



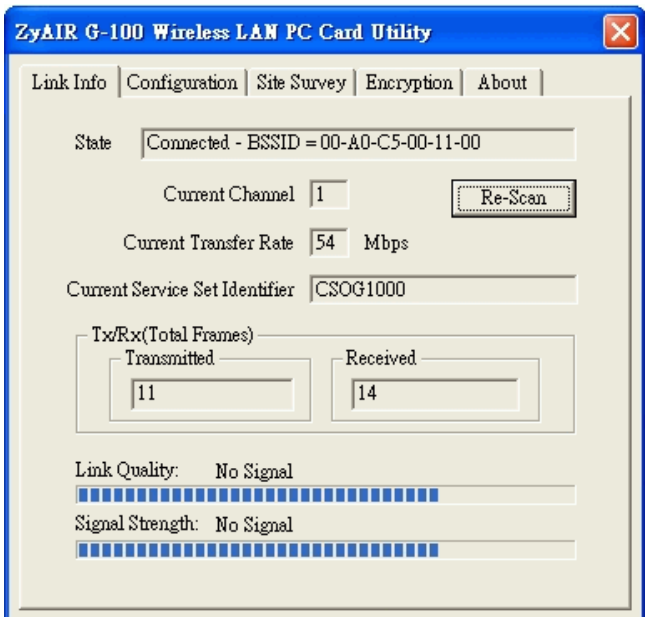
Key settings

Enter exactly 5, 13 or 29 characters for the 40/64bit, 128-bit, 256-bit WEP keys respectively.

WEP Key Configuration on the Wireless Client

1. Double-click on the ZyXEL utility icon in the system tray or right-click on the utility icon and select 'Show Config Utility'.

The utility screen displays.



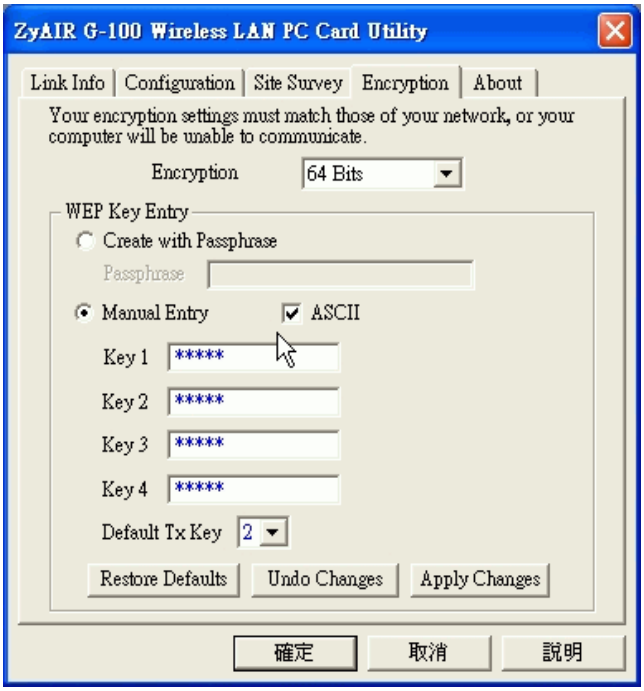
Note: If the utility icon is not in the system status, click Start > Programs > IEEE802.11b WLAN Card > IEEE802.11b WLAN Card to display the utility screen.

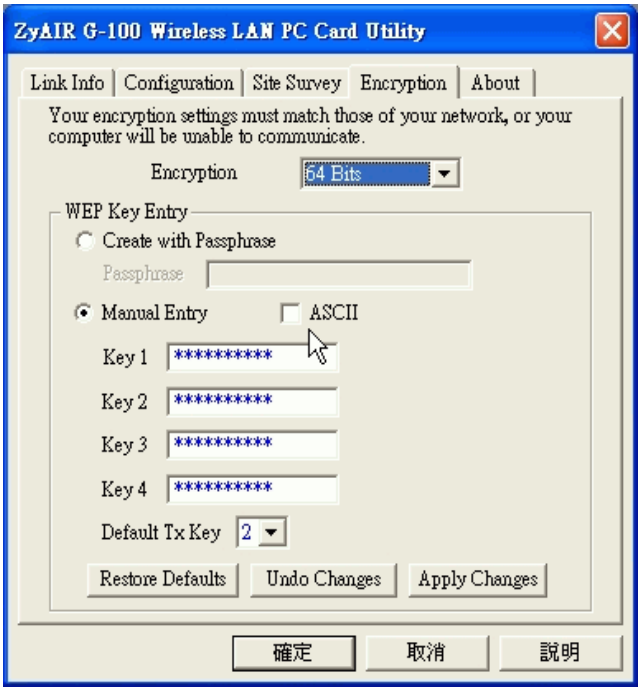
2. Click the **Encryption** tab.

Select the same encryption type as the access point.

Configure the same four WEP keys as the access point.

Select a WEP key as the default key to use for data encryption in the wireless LAN.





WEP Key Setup

You must use the same WEP keys on the wireless clients and the access point.

To enter ASCII characters for the WEP keys, select **ASCII**. Otherwise clear the **ASCII** check box and enter hexadecimal characters starting with '0x'.
For example,

64-bits ASCII WEP key :
Key1= 2e3f4
Key2= 5y7js
Key3= 24fg7
Key4= 98jui

64-bits hexadecimal WEP key :
Key1= 123456789A
Key2= 23456789AB
Key3= 3456789ABC
Key4= 456789ABCD

Site Survey

Introduction

What is Site Survey?

In a wireless network, it is difficult to predict the propagation of radio waves and detect the presence of wireless devices in the same wireless network. Concrete walls, buildings, and natural obstacles reduce wireless signal quality and increase attenuation. These result in irregular FR coverage patterns.

With the Site survey feature, you can easily detect wireless devices within transmission range.

Preparation

The following procedure describes how to prepare your network environment to use a simple site survey tool.

1. Obtain a blueprint of the location or building where the wireless network is to be installed. The blueprint allows you to mark points of interest.

2. Visually inspect the location. Walk around the location to verify the accuracy of the blueprint and mark any large obstacles you see that may affect RF signals. These obstacles include things like metal shelf, metal desk, or concrete walls.

3. Identify where most users are located. Inquire where the users intend to use or install the wireless network and also where wireless coverage is not required. This allows you to determine how many APs are needed.

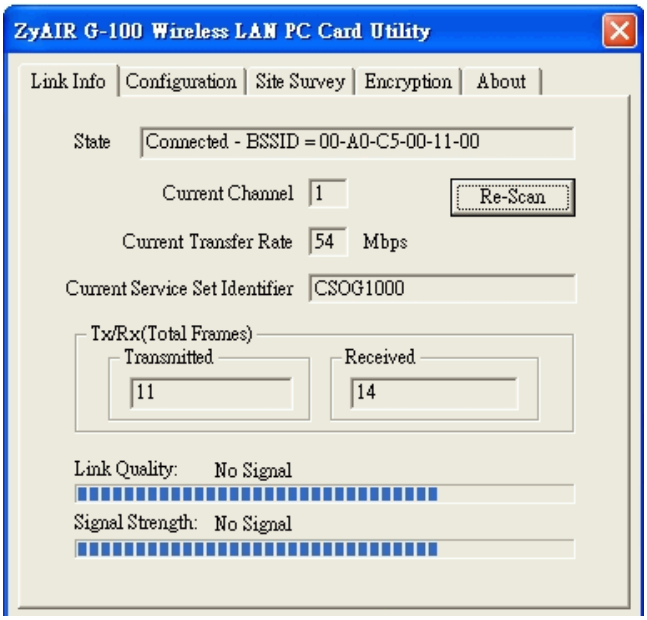
4. Determine the preliminary access point location on blueprint based on the service area needed, obstacles and the locations of power wall jacks.

Survey on the Site

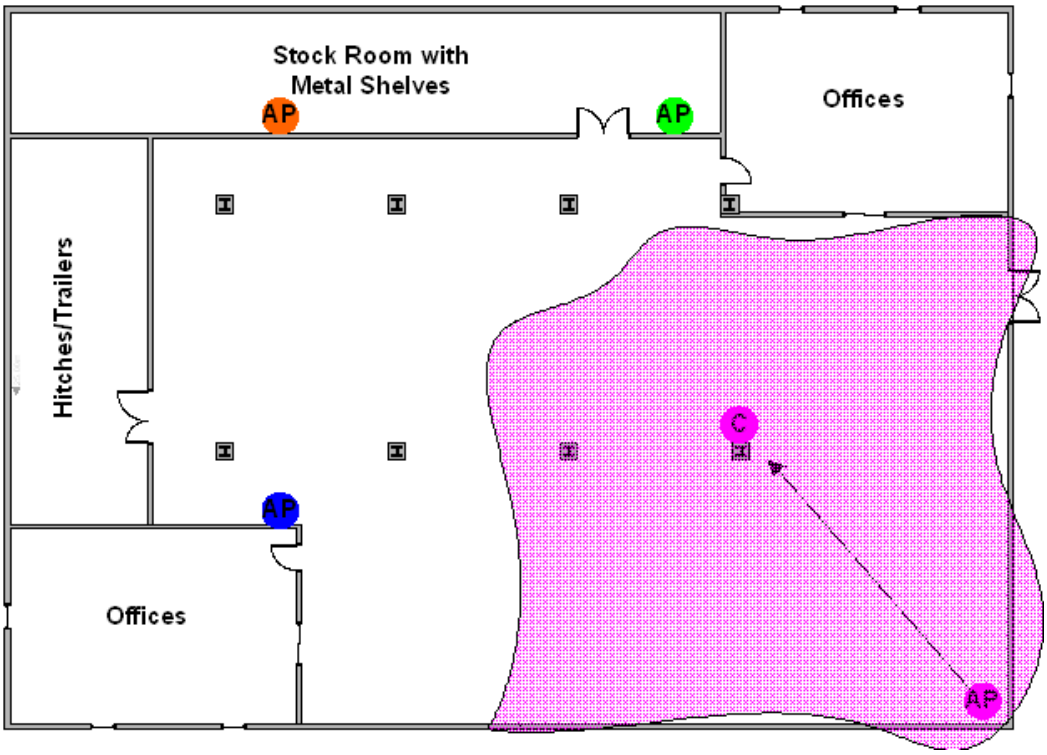
1. You should have the blueprint with all the information obtained during the preparation phase. Now you are ready to do the site survey.

2. Install an access point at a preliminary location.

3. Use a notebook with a wireless client adapter installed, run the site survey utility and walk around the AP. The site survey should detect and display wireless information such as connection speed, current used channel, associated rate, link quality, signal strength, etc..



4. It's always a good idea to start with putting the AP at one corner of the room and walk away from the AP. Record down the changes at the point where the transfer rate drops dramatically and also the link quality and signal strength information on the diagram as you go alone.

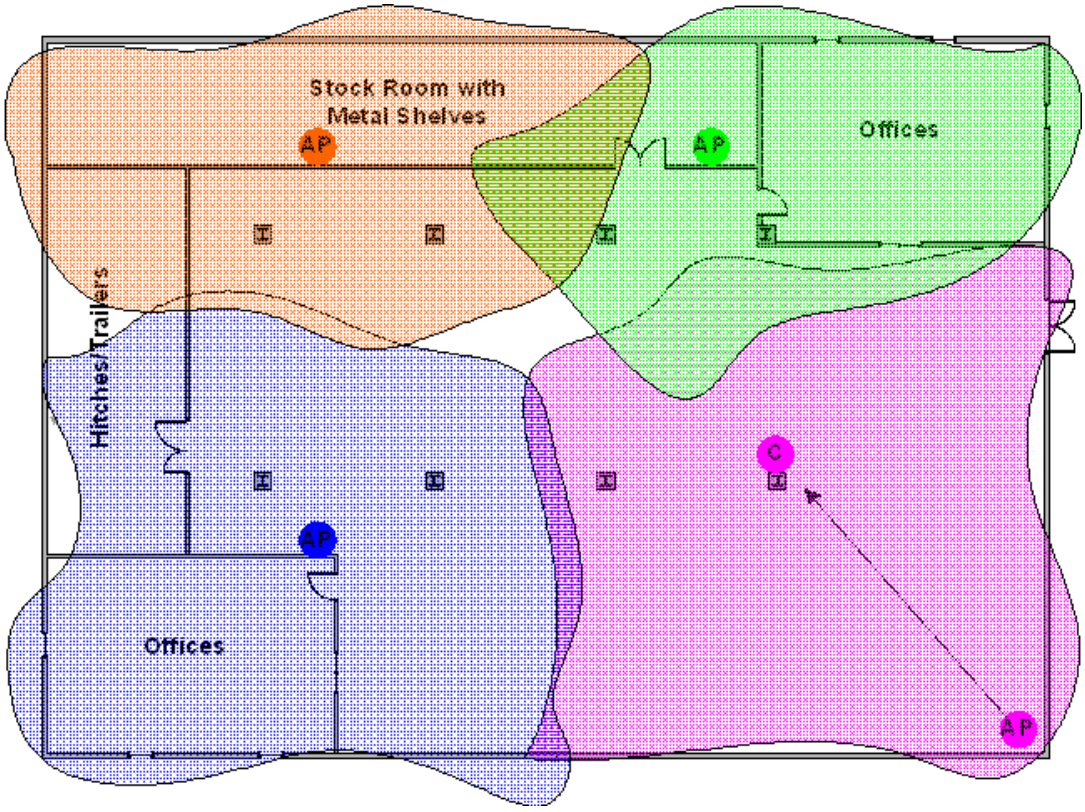


5. When you reach the farthest distance from the AP and can still retain a reasonable wireless connection, mark the point. This is the wireless coverage boundary point. Then move the AP to this new location marked as the boundary of the original wireless coverage area.

6. Repeat steps 1~5. You should be able to map the RF coverage area as illustrated in above picture.

7. The markings determine how many APs you need to provide full wireless coverage in the area.

8. Repeat steps 1~6 for any rooms in the location. Once completed, you should have a complete wireless network mapping as shown in the example figure below.



Note: If you want to install more than one AP in the area, make sure adjacent wireless coverage areas overlap slightly on the boundary. This allows the wireless clients to seamlessly roam between coverage areas.

PSTN Lifeline Application Notes

Usage of PSTN Lifeline

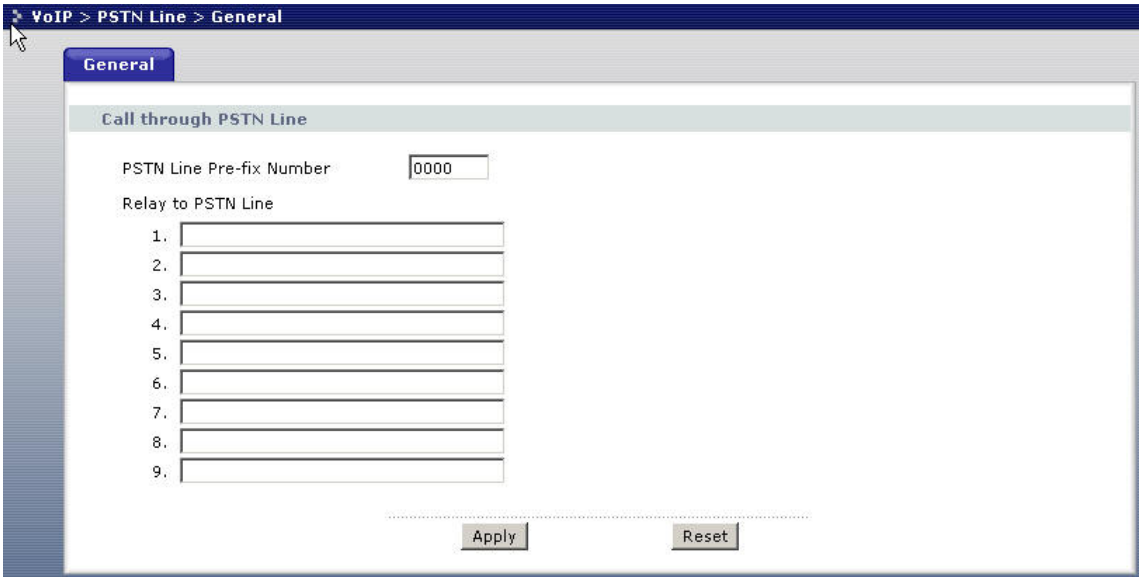
With the PSTN lifeline function, you can make and receive regular PSTN phone calls in concurrently while using VoIP services on the same phone. This can be done by simply assigning a prefix number (by default the prefix for PSTN dial out is 0000 and is configurable) for making a PSTN call. When you dial this prefix number, the device automatically uses the PSTN line for making the regular PSTN call.

Furthermore, when power to the Prestige is cut during natural disasters (such as earthquake or hurricane), it automatically switch to use the PSTN line for phone calls without you having to enter the prefix number.

This lifeline feature also allows you to still make phone calls during emergency situations such as contacting the police, the fire department or emergency medical services during a power outage. The following section shows you how to set up the lifeline support feature on the Prestige using the web configurator.

Lifeline configuration

To configure the lifeline feature on the Prestige, click VoIP > PSTN Line in the navigation panel to display the configuration screen as shown next.



In the **PSTN Line Pre-fix Number**, enter the special prefix number used to set the Prestige to switch from VoIP to the PSTN system when making a regular PSTN call. For example, when you want to dial out to a PSTN destination, first pick up the phone (you should heard a dial tone), and enter the specified prefix number (in this case, 0000). You will hear the dial tone again. At this point, you can dial out to PSTN as you would on a regular PSTN system.

Relay to PSTN

The Relay to PSTN field can be found under PSTN configuration WEB GUI in **Relay to PSTN** section. This field is used to specify phone numbers to which the Prestige will always send calls through the regular PSTN phone service without pushing prefix. In other words, numbers which specify on this field do not need to dial prefix number to be dialed out. However, these numbers must be for phones on the PSTN (not VOIP phones) and currently, P2608HWL Series support up to nine entries under this field.

After configuring the PSTN setup, click “Apply” to save changes back to P2608HWL.

Note: It is recommended to configure your local emergency services such as Police Dept, Fire Dept, and Emergency Medical services phone number in this field. Thus in any cases, these unit can be reach in case of emergency by dialing their number without prefix, regardless if there are power loss.

How to connect Lifeline and DSL connection

To use both VOIP and regular phone service with P2608HWL’ s lifeline feature. You will need to connect ADSL line and phone line appropriately and make proper configuration.

Making the correct connection it allows you to still receive phone calls while someone else is making outgoing VoIP call though Prestige’ s 8 pots port, the following figure shows you how to connect your phone and DSL service.

If your ADSL line type is Splitter type you ISP will provide you with splitter otherwise it should be splitterless. For correct info you may check with your service provider as for which type of line you have.

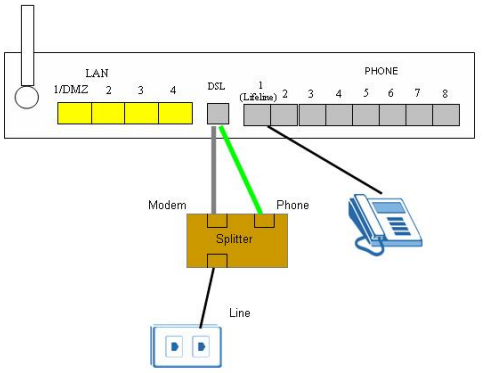


Figure 1 Splitter type

1. The P2608HWL Series includes a DSL cable and a RJ-11 cable. Connect the DSL cable to the DSL port and connect RJ-11 to Lifeline port.
2. Connect the RJ11 to the splitter **phone** jack or a telephone wall jack
3. Connect the DSL cable to the splitter **modem** jack or ADSL line
4. Connect the splitter jack where it labels **Line** to ADSL line from the ISP.

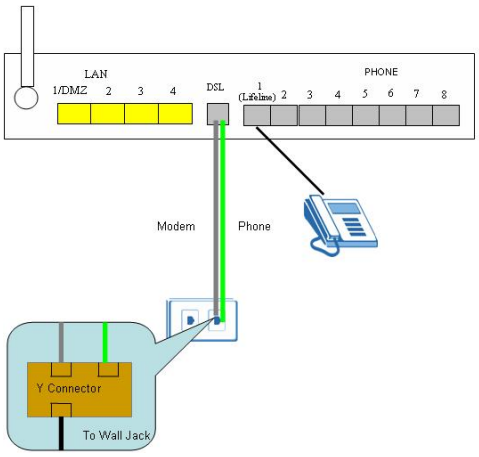


Figure 2 Splitterless type

1. The P2608HWL Series includes a DSL cable and a RJ-11 cable. Connect the DSL cable to the DSL port and connect RJ-11 to Lifeline port.
2. You need to obtain a regular PSTN Y connector from regular phone shop.
3. Connect the RJ-11 to one of the output jack on the Y connector
4. Connect the DSL cable to the other output jacket on the Y connector
5. Connect the Y connector input port with a phone cable to the wall Jack or line from ISP.

VoIP Application Notes

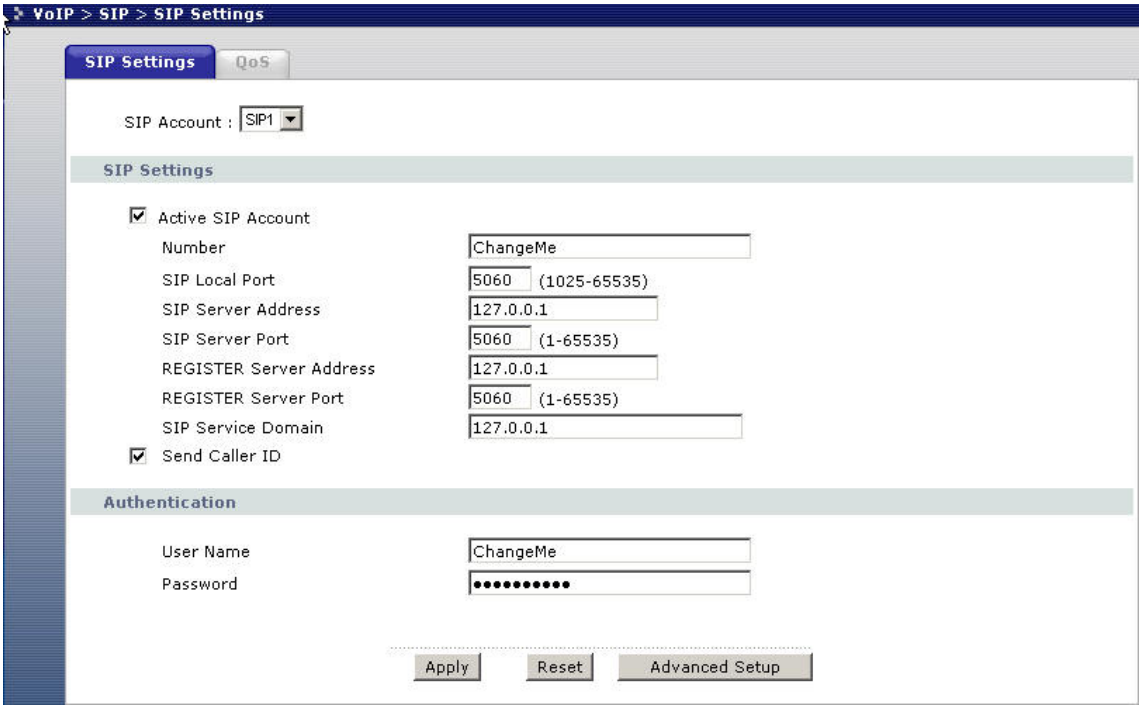
SIP Account Setup

VoIP is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send fax 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 eight SIP accounts simultaneously. Follow the procedure below to configure SIP accounts.

Note: You should have a voice account already set up and have VoIP information from your VoIP service provider prior to configuring the SIP account on to 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. Click Apply to save the settings. If you want to configure a second SIP account, select SIP2 in the SIP Account field and follow steps 1 – 6.

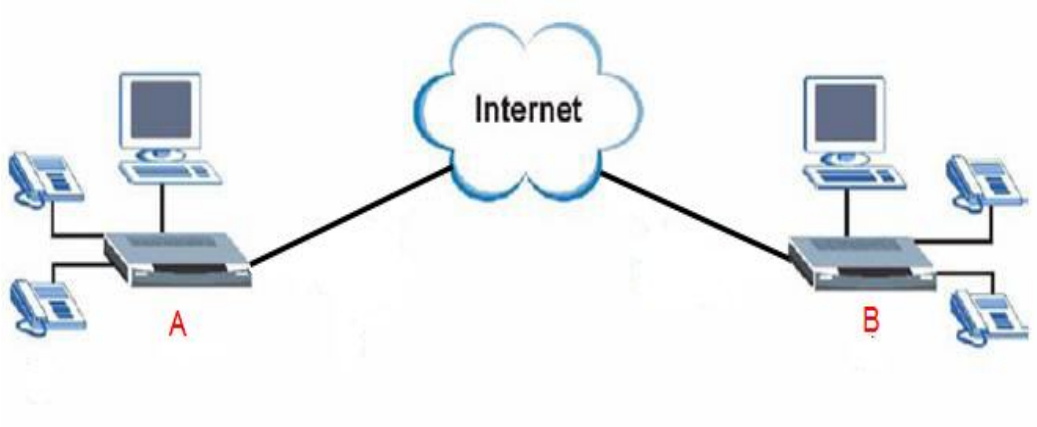
The following table describes the screen labels.

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.
User Name	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.
Password	Type the password associated with the user name above. Use ASCII Extended set characters.
Send Caller ID	Select this check box to show identification information when you make VoIP calls. Clear this check box to not show identification information when you make VoIP calls.
Advanced Setup	Click **Advanced Setup** 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.

Peer to Peer call

Topology



Network Topology

1. Devices A and B are placed at different locations over the Internet.
2. The public IP address of devices A and B are 220.130.46.197 and 220.130.46.198 respectively.
3. SIP number for device A is 197 and for devices B is 198.

Configuration Preparation and Steps

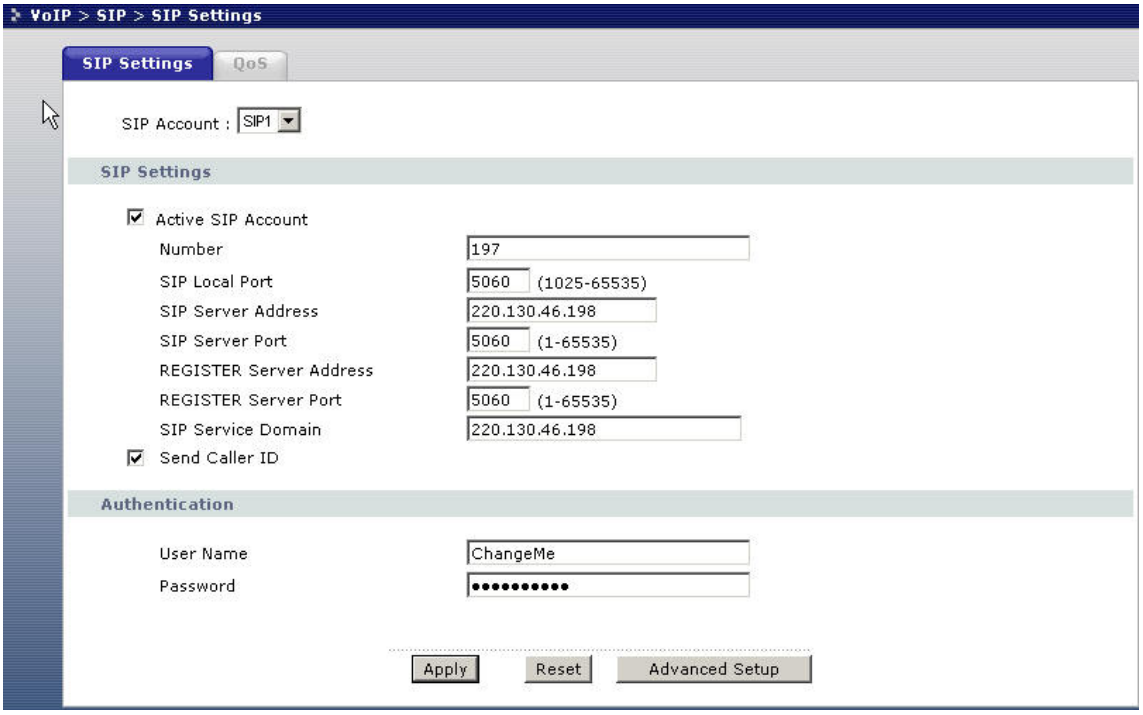
1. Install the devices in the network.
2. Set up the devices' WAN connections.
3. Configuring SIP / VoIP related settings in devices A and B.

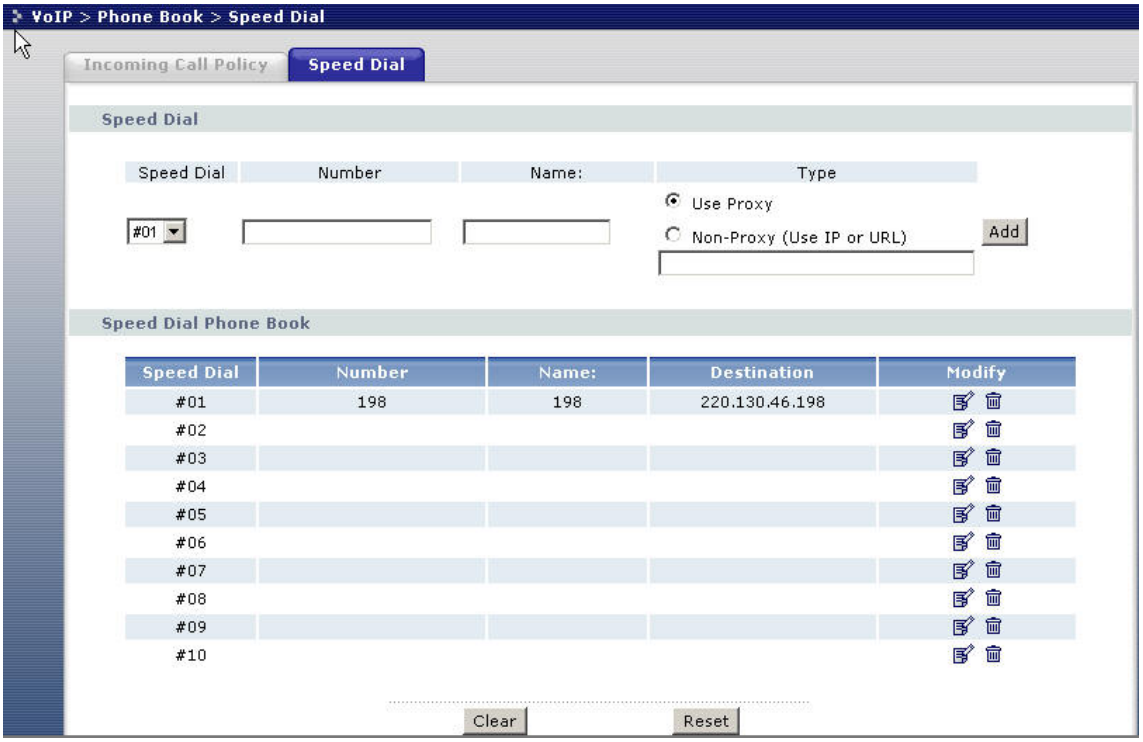
There are two ways to make an IP-to-IP call.
(1) Make a call using a speed dial number (like '#01') defined in the phone book.
You need to configure the your SIP number in the VoIP configuration screen and the callee's IP address in the phone book

Note that there are you can specify up to 10 speed dial numbers on the Prestige.

(2) Make a call using the caller's SIP number
You need to configure the your SIP number and specify the address of the caller, SIP server, SIP proxy, Domain server in the VoIP configuration screen.

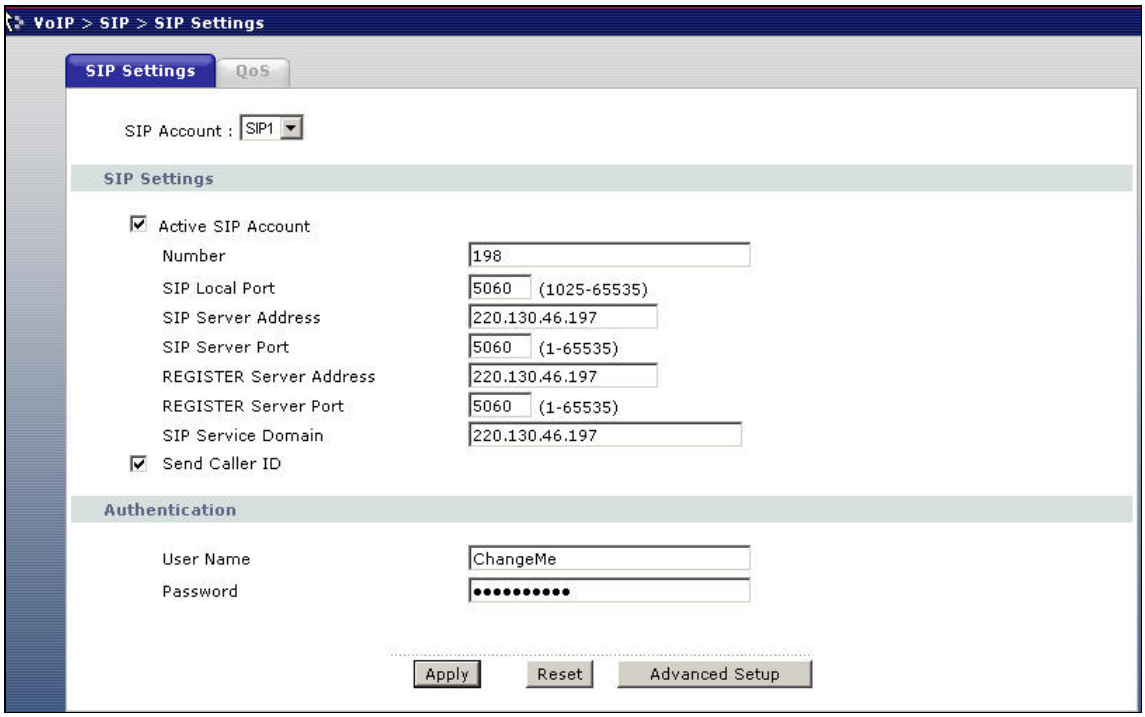
Setup--- Configuring SIP / VoIP related settings in device A

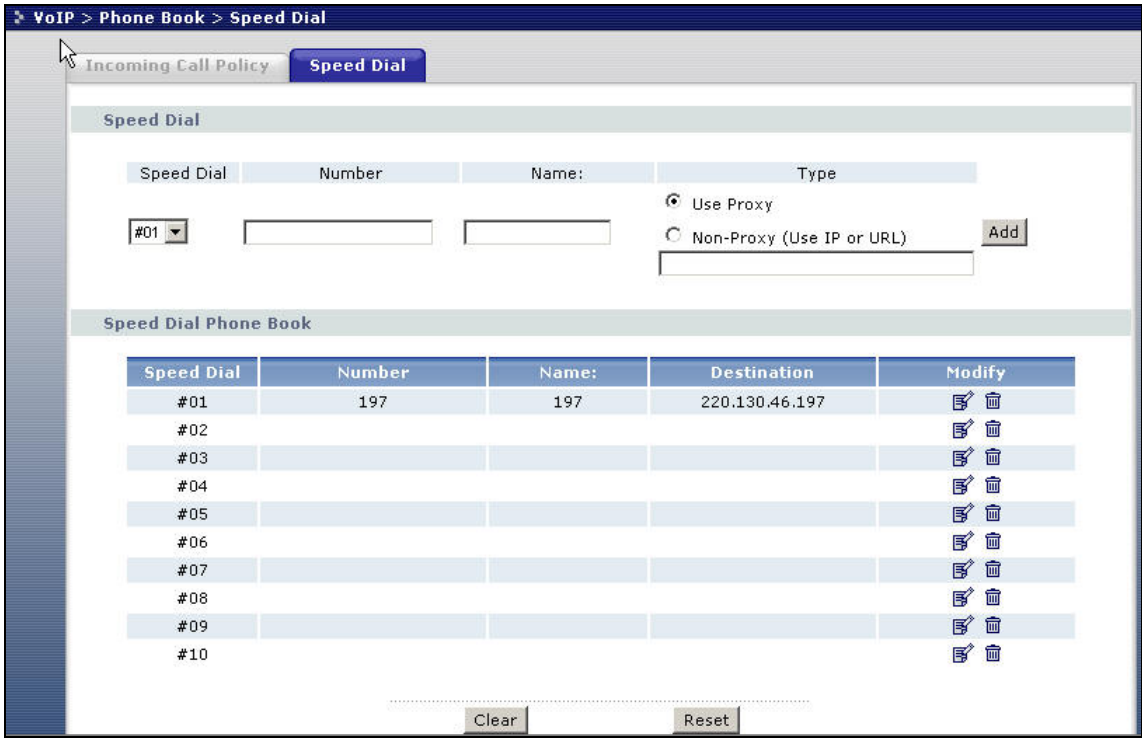




1. In the VoIP web configurator screen, enter device A's number in the SIP number column.
2. Enter the IP address of device B as the SIP server address, Register server address (as shown in this example).
3. Set up the speed dial. Enter the information of device B in the column.

Setup--- Configuring SIP / VoIP related settings in device B





1. In the VoIP web configurator screen, enter device B's number in the SIP number column.
2. Enter the IP address of device A as the SIP server address, Register server address (as shown in this example).
3. Set up the speed dial. Enter the information of device A in the column.

After you have configured the settings, you can dial #01 on the phone behind device A. The phone behind device B should ring.

Phone Port Settings

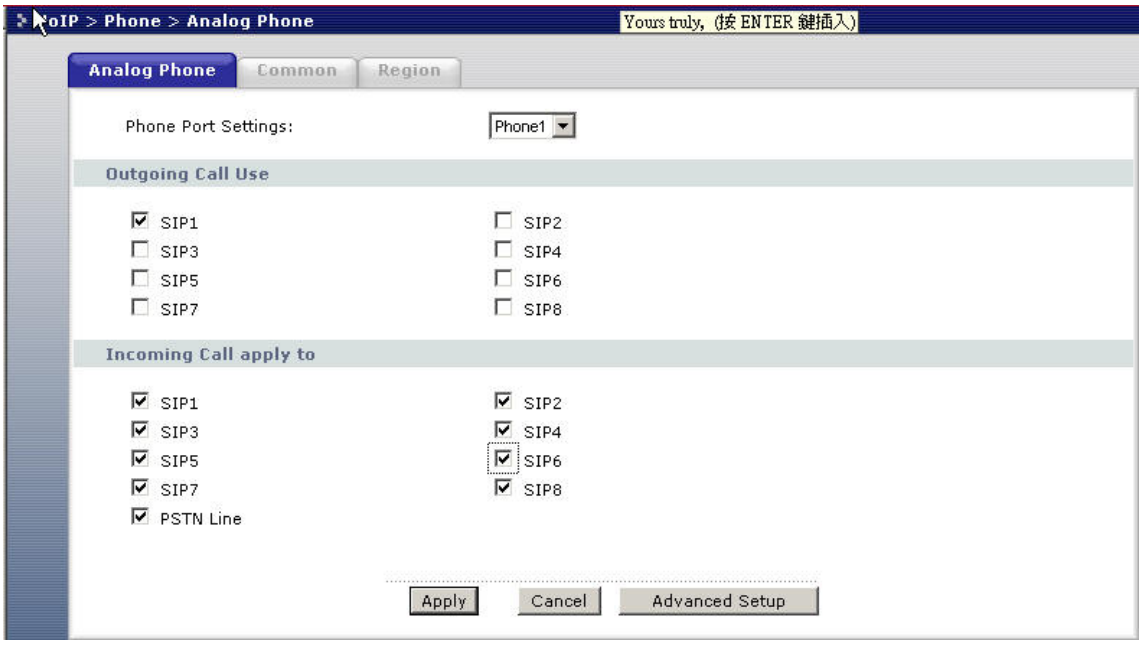
Prestige allows you to configure the volume and echo cancellation setting for each individual phone port.

Analog Phone Configuration

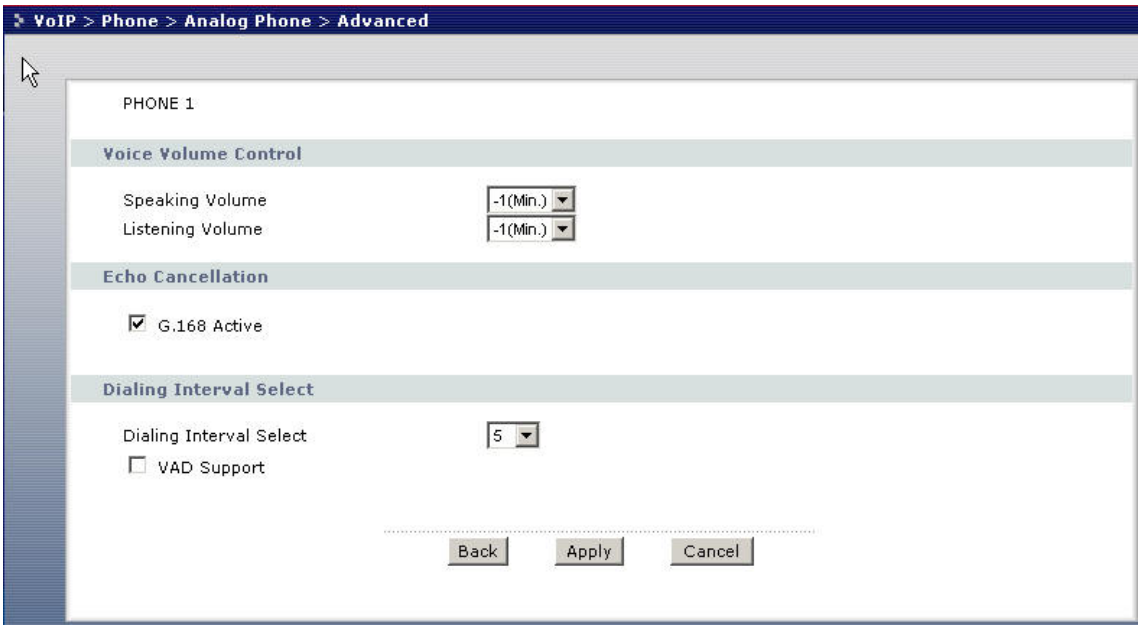
Outgoing Call Use -
You can set the Prestige to use the analog phone for the selected SIP account(s) for outgoing calls.

Incoming Call apply to -

For incoming calls, you can specify the SIP account(s) and the line type. For example, if you select SIP1 for the incoming call in this screen and a person dials the SIP1 number from a remote end, all of your analog phone will ring.



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



Follow the steps below to configure To configure the phone port setting, please follow the below steps:

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 > Advanced Setup** to display the configuration screen.

Step 4. Set the phone port parameters and click **Apply** to save the settings and make the changes take effect.

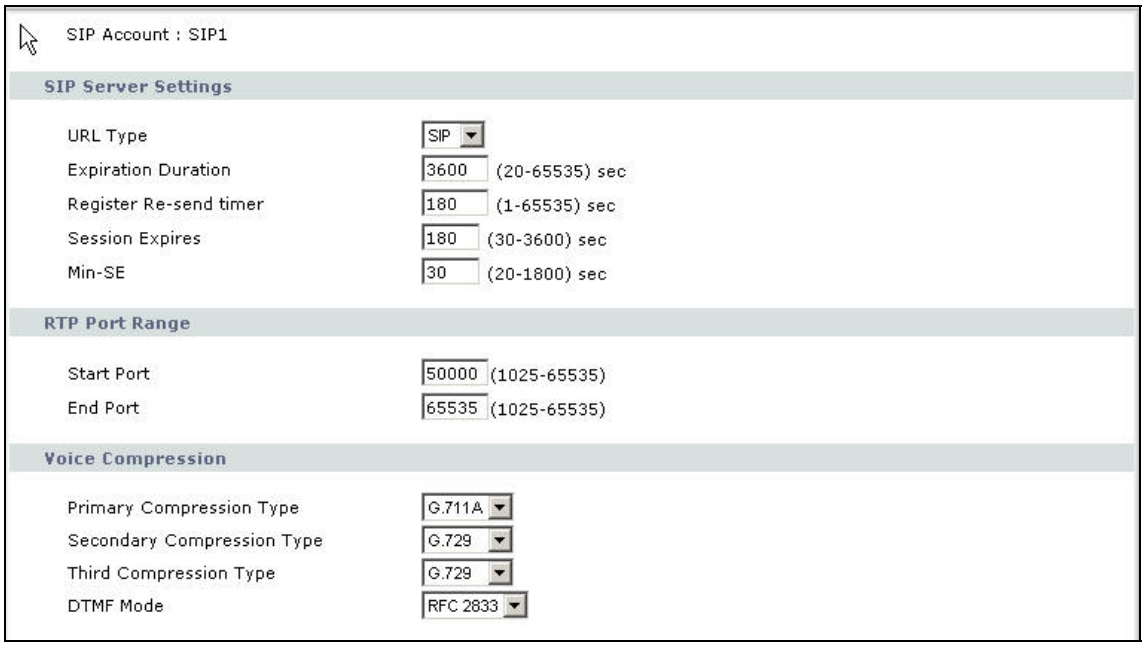
The table below describes the related fields.

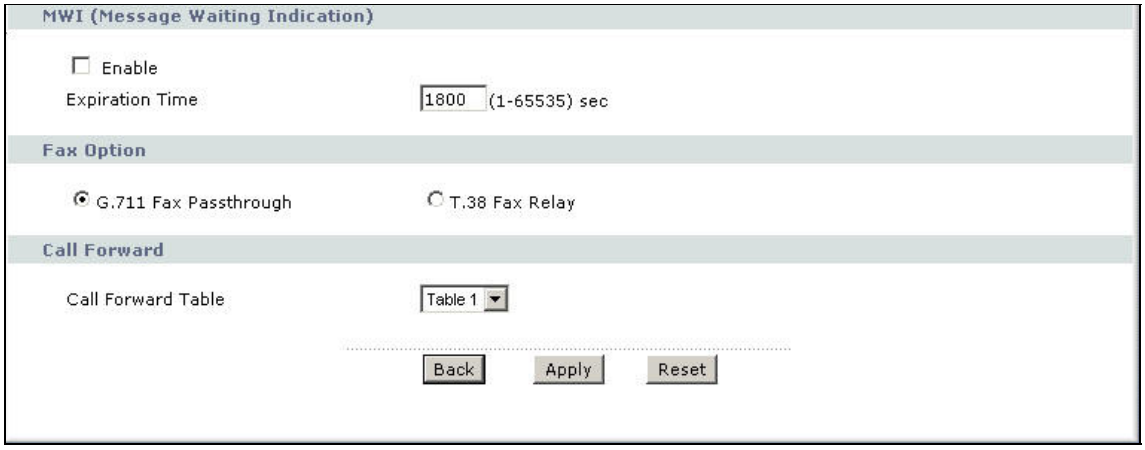
Label	Description
Speaking Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it sends to the peer device. -1 is the quietest and 1 is the loudest.
Listening Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it receives from the peer device and sends to your phone. -1 is the quietest and 1 is the loudest.

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.

Configuring Advanced Voice Settings

In the web configurator, click **VoIP** > **SIP** to open the **SIP Settings** screen. Select a SIP account to configure and then click **Advanced Settings** to display the following screen. Use this screen to change SIP server, RTP port range, preferred compression type (codec), DTMF type and Message Waiting Indication (MWI) settings.





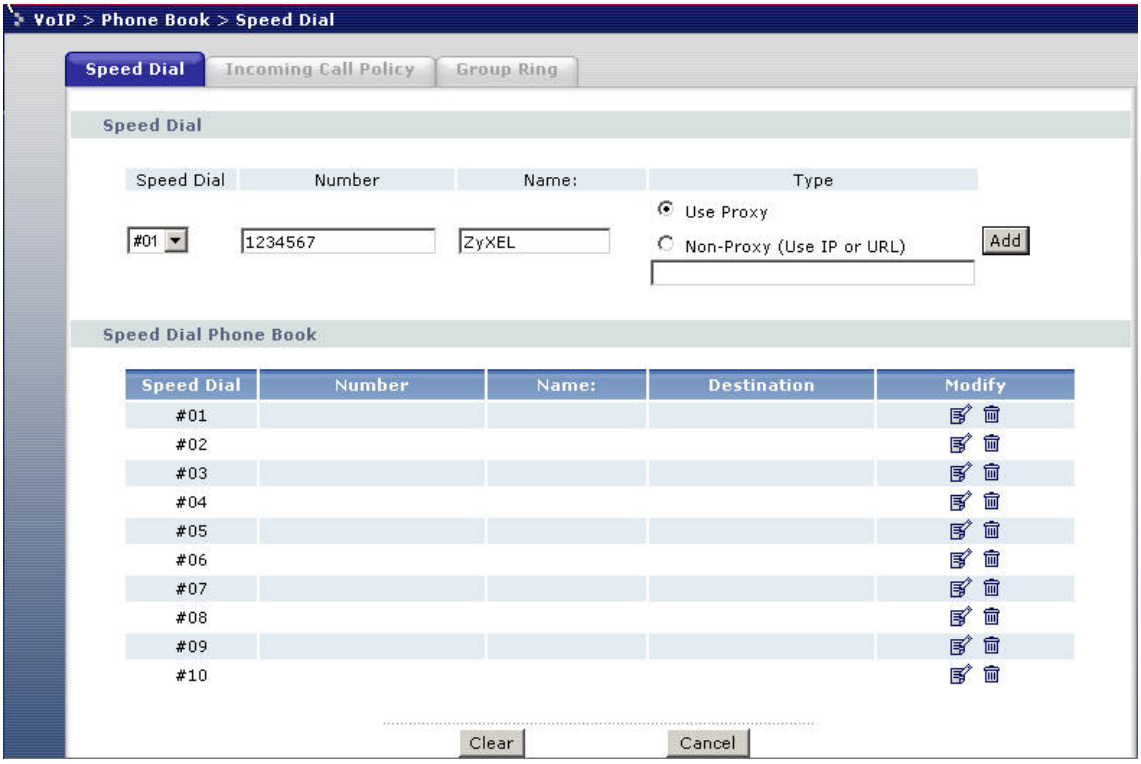
The table below describes the fields in this screen.

Label	Description
SIP Account	This read-only field displays the number of the SIP account that you are configuring. The changes that you save in this page affect the Prestige's settings with the SIP account displayed here..
URL Type	Select **SIP** to have the Prestige include the domain name with the SIP number in the SIP messages that it sends. Select **TEL** to have the Prestige use the SIP number without a domain name in the SIP messages that it sends.
Expiration Duration	This field sets how long an entry remains registered with the SIP register server. After this time period expires, the SIP register server deletes the Prestige's entry from the database of registered SIP numbers. The register server can use a different time period. The Prestige sends another registration request after half of this configured time period has expired.
Register Re-send Timer	Use this field to set how long the Prestige waits before sending a repeat registration request if a registration attempt fails or if there is no response from the registration server.
Session Expires	Use this field to set the longest time that the Prestige will allow a SIP session to remain idle (without traffic) before dropping it
Min-SE	When two SIP devices negotiate a SIP session, they must negotiate a common expiration time for idle SIP sessions. This field sets the shortest expiration time that the Prestige will accept. The Prestige checks the session expiration values of incoming SIP INVITE requests against the minimum session expiration value that you configure here. If the session expiration of an incoming INVITE request is less than the value you configure here, the Prestige negotiates with the other SIP device to increase the session expiration value to match the Prestige's minimum session expiration value.
RTP Port Range	Real time Transport Protocol (RTP) is used to handle voice data transfer. Use this field to configure the Prestige's listening port range for RTP traffic. Leave these fields set to the defaults if you were not given a range of RTP ports to use.

DTMF Mode	The Dual Tone Multi-Frequency (DTMF) mode sets how the Prestige handles the tones that your telephone makes when you push its buttons. It is recommended that you use the same mode that your VoIP service provider uses. Select **RFC 2833** to send the DTMF tones in RTP packets. Select **PCM** (Pulse Code Modulation) to include the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) could distort the tones. Select **SIP INFO** to send the DTMF tones in SIP messages.
MWI (Message Waiting Indication)	Enable Message Waiting Indication (MWI) to have your phone give you a message–waiting (beeping) dial tone when you have a voice message. Your voice service provider must have a messaging system that supports this feature.
Expiration Time	Use this field to set how long the SIP server should continue providing the message waiting service after receiving a SIP SUBSCRIBE message from the Prestige. The SIP server stops providing the message waiting service if it has not received another SIP SUBSCRIBE message from the Prestige before this time period expires.
Call Forward Table	Select which call-forwarding table you want the Prestige to use to block or redirect calls. You can use a different call-forwarding table for each SIP account or use the same call-forwarding table for both.
Back	Click **Back** to return to the previous screen without saving configuration changes.
Apply	Click **Apply** to save your changes back to the Prestige.

Speed dial Phone book

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 phone book for speed dialing.

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.

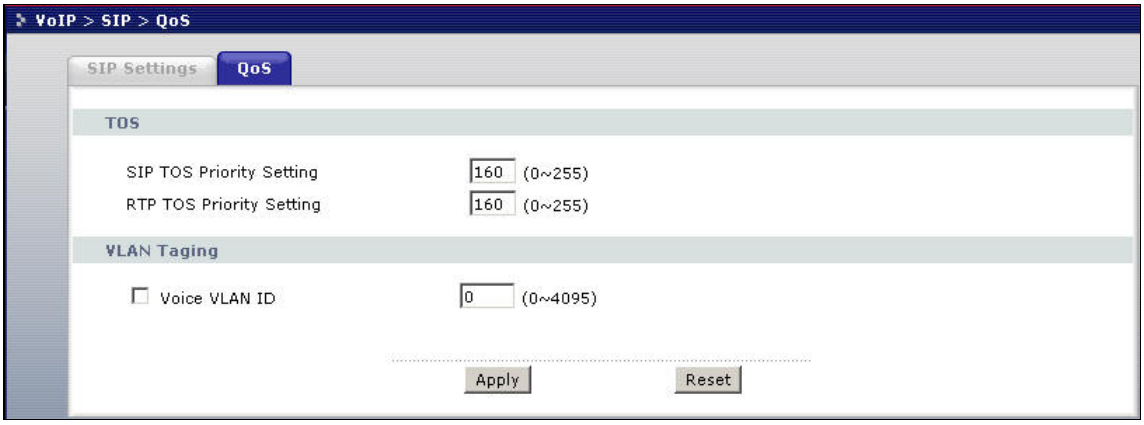
Step 6. Click **Add** to save the entry to the phone book.

The table below describes the fields in this screen.

Label	Description
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.

Voice - QoS setup

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications. Click **VoIP > SIP-> QoS** to display the following screen.



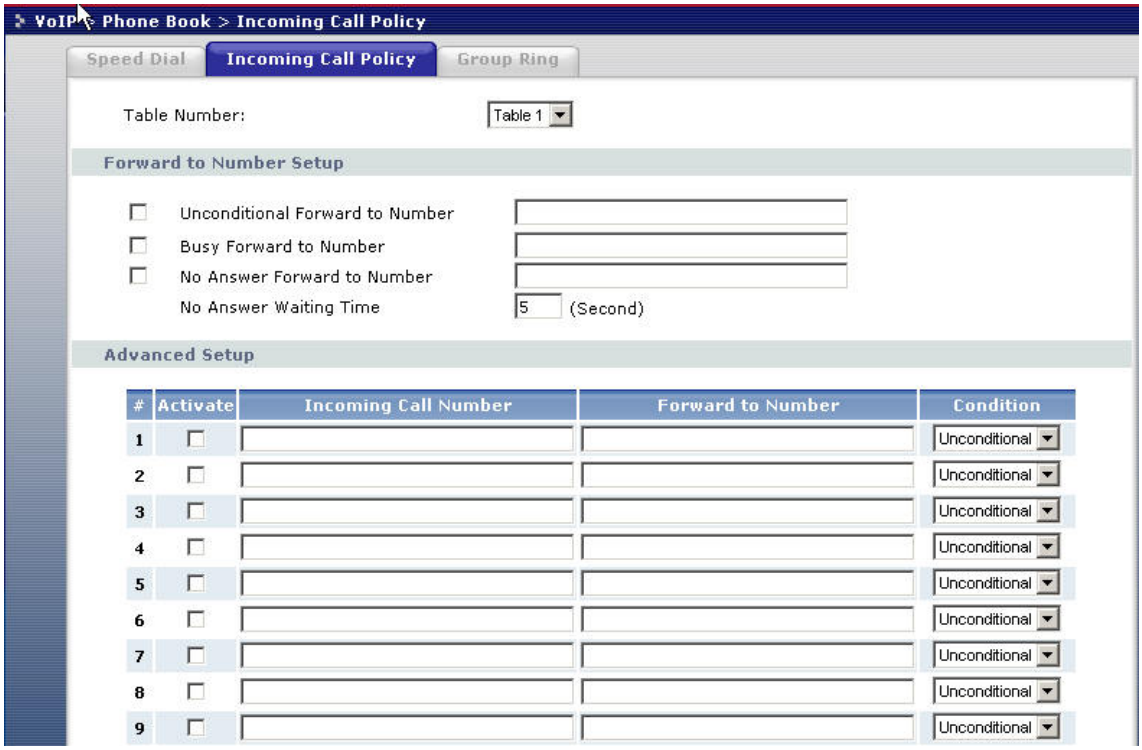
The table below describes the fields in this screen.

Label	Description
SIP TOS Priority	Type a priority for voice transmissions. The Prestige includes the Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority	Type a priority for voice transmissions. The Prestige includes the Type of Service priority tags with this priority to RTP traffic that it transmits.
Voice VLAN ID	Enable VLAN tagging if the Prestige needs to be a member of a VLAN group in order to communicate with the SIP server. Your LAN and gateway must also be set up to use VLAN tags. Some switches also give priority to voice traffic based on its VLAN tag. Type the VLAN ID (VID) from 1 to 4095 for the Prestige to add to voice Ethernet frames that it sends out. Disable VLAN tagging if the Prestige does not need to be a member of a

	VLAN group to communicate with the SIP server.
Apply	Click **Apply** to save your changes back to the Prestige.

Call Forwarding Setup

Configure the call forwarding function on the Prestige to handle incoming calls. For example, you may decide that all incoming calls will also ring your cell phone. You can also use the Prestige to block or redirect calls using call forwarding. You can set the Prestige to use a different call-forwarding table for each SIP account or use the same call-forwarding table for both SIP accounts.



Unconditional Forward to Number

Enable this feature to have the Prestige forward incoming calls to the number that you configure.

Busy Forward to Number

Enable this feature to have the Prestige forward incoming calls to the number that you configure when your SIP account has a call connected.

No Answer Forward to Number

Enable this feature to have the Prestige forward incoming calls to the number that you configure whenever you do not answer the call after a specific time period.

The table below describes the fields in this screen.

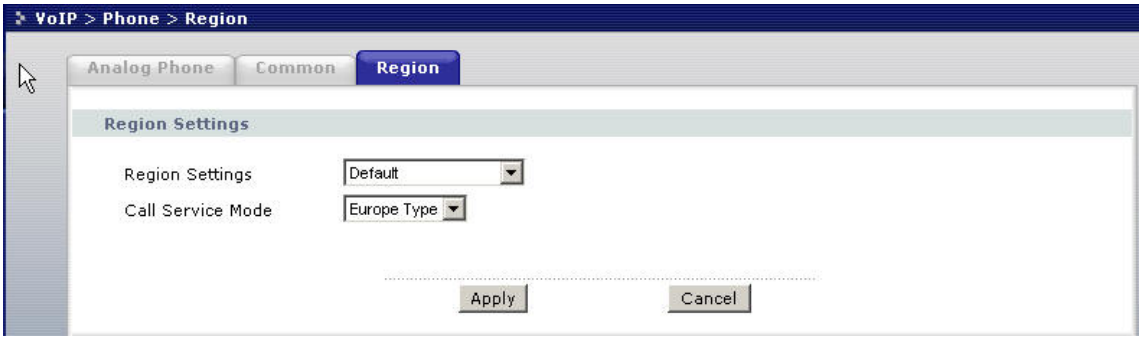
Label	Description
Table Number	Select which call forwarding table you want to configure. You can configure a different call forwarding table for each SIP account or use the same call forwarding table for both.
	The following applies to the number fields in this screen. For a SIP number, use the number or text that comes before the @ symbol in a full SIP URI.
Forward to Number Setup	These are the global call forwarding settings that define the default action to take on incoming calls that do not match any of the **Advanced Setup** call forwarding entries.
Unconditional Forward to Number	Enable this feature to have the Prestige forward all incoming calls to the number that you configure regardless of whether or not the phone(s) connected to the phone port(s) is busy.
Busy Forward to Number	Enable this feature to have the Prestige forward incoming calls to the number that you configure when the phone(s) connected to the phone port(s) is busy. With call waiting, a second call is only forwarded after being rejected.
No Answer Forward to Number	Enable this feature to have the Prestige forward incoming calls to the number that you configure whenever you do not answer the call after a specific time period.

No Answer Waiting Time	Set how long the Prestige should let a call ring before considering the call unanswered.
Advanced Setup	Configure **Advanced Setup** call forwarding entries to have the Prestige perform specific actions on calls from specific numbers. If a caller's number does not match any **Incoming Call Number** entries, the Prestige performs the default action configured in the **Forward to Number Setup** section.
Activate	Select this check box to enable a call forwarding entry.
Incoming Call Number	You can set the Prestige to take a particular action on incoming calls from a number that you specify here.
Forward to Number	You can set the Prestige to forward incoming calls to a number that you specify here.
Condition	Select under what circumstances you want the Prestige to use this call forwarding entry. Select **Unconditional** to have the Prestige immediately forward a call from the number specified in the **Incoming Call Number** field to the number in the **Forward to Number** field. Select **Busy** to have the Prestige forward a call from the number specified in the **Incoming Call Number** field to the number in the **Forward to Number** field when your SIP account has a call connected. Select **No Answer** to have the Prestige forward a call from the number specified in the **Incoming Call Number** field to the number in the **Forward to Number** field when the **No Answer Waiting Time** period expires (whether or not the no answer feature is enabled in the **Forward to Number Setup** section). Select **Block** to have the Prestige reject calls from the number specified in the call forwarding entry. Select **Accept** to have the Prestige allow calls from the number specified in the **Incoming Call Number** field.

Voice – Common Settings

Click **VoIP > Phone > Common** to display the configuration screen. Use this screen to enable or disable the Immediate Dial function.

Click **VoIP > Phone > Region** to display the following screen. Use this screen to configure common VoIP Settings.



The table below describes the fields in this screen.

Label	Description
Region Settings	Use the drop-down list box to select the country where your Prestige is located.
Immediate Dial	Use these fields to specify phone numbers to which the Prestige will always send calls through the regular phone service without the need of dialing a prefix number. These numbers must be for phones on the PSTN (not VoIP phones).
Call Service Mode	Use this field to set how the Prestige handles supplementary phone services (call hold, call waiting, call transfer and three-way conference calls). Select

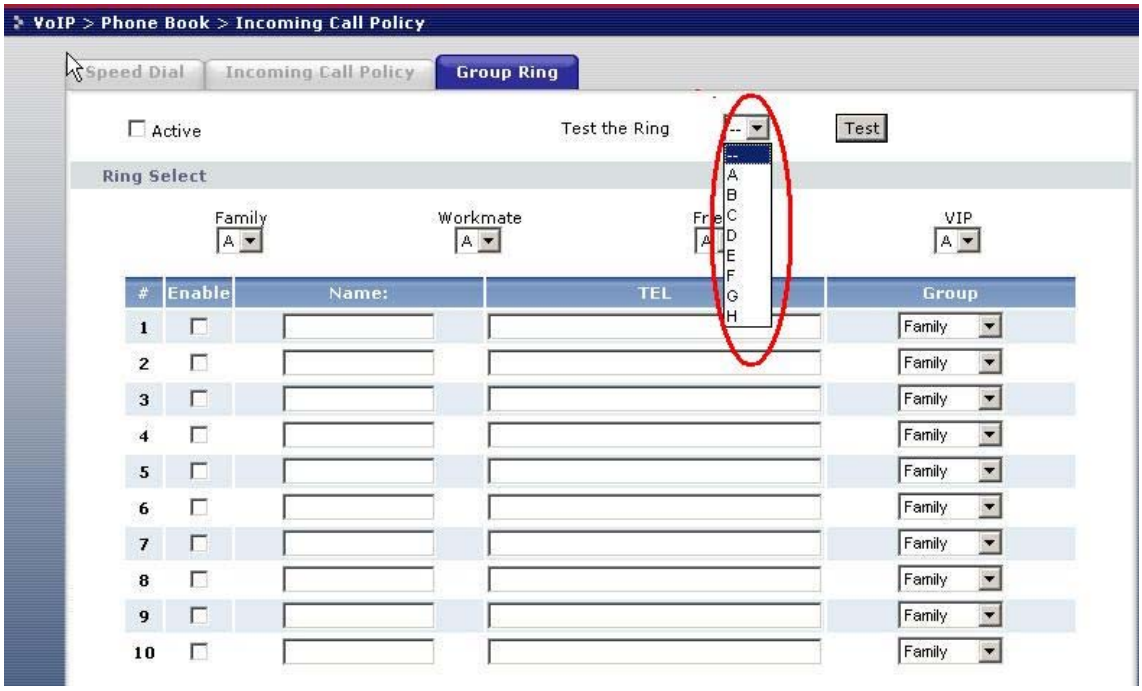
	the mode that your voice service provider supports. Select **Europe Type** to use the supplementary phone services in European mode. Select **USA Type** to use the supplementary phone services American mode. See your User's Guide for supplementary phone service details. **To take full advantage of the supplementary phone services available through the Prestige's phone ports, you may need to subscribe to the services from your voice service provider.**
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.

Group Ring

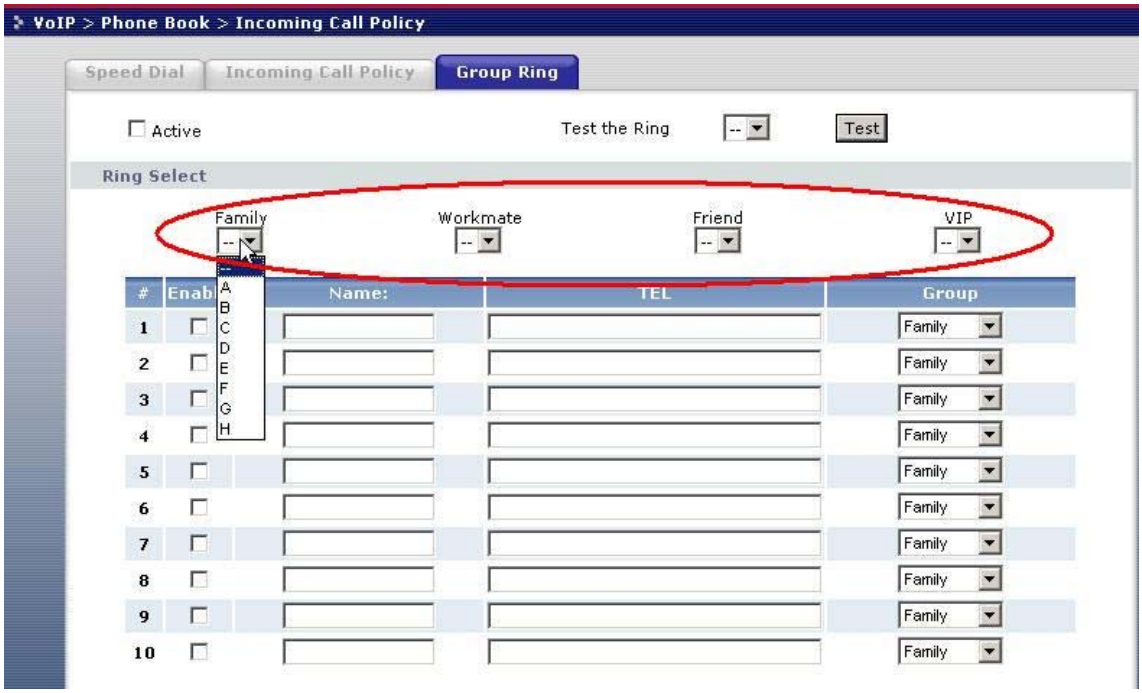
Group Ring can help user to identify where the incoming call come from (SIP, predefined group, PSTN…etc) by specifying a distinctive ring to each group. User can use WEB GUI to configure this feature. User must set the different phone number in the table shown below and then select a special ring tone from type A to type H for each group. After successfully configure the group ring, the incoming call will have distinctive ring for each group. If the incoming phone number is not in the table, it will ring based on where it comes from (SIP1 ~ SIP 8, PSTN, Internal Call)

Below are the screenshots to explain the usage of this particular feature.

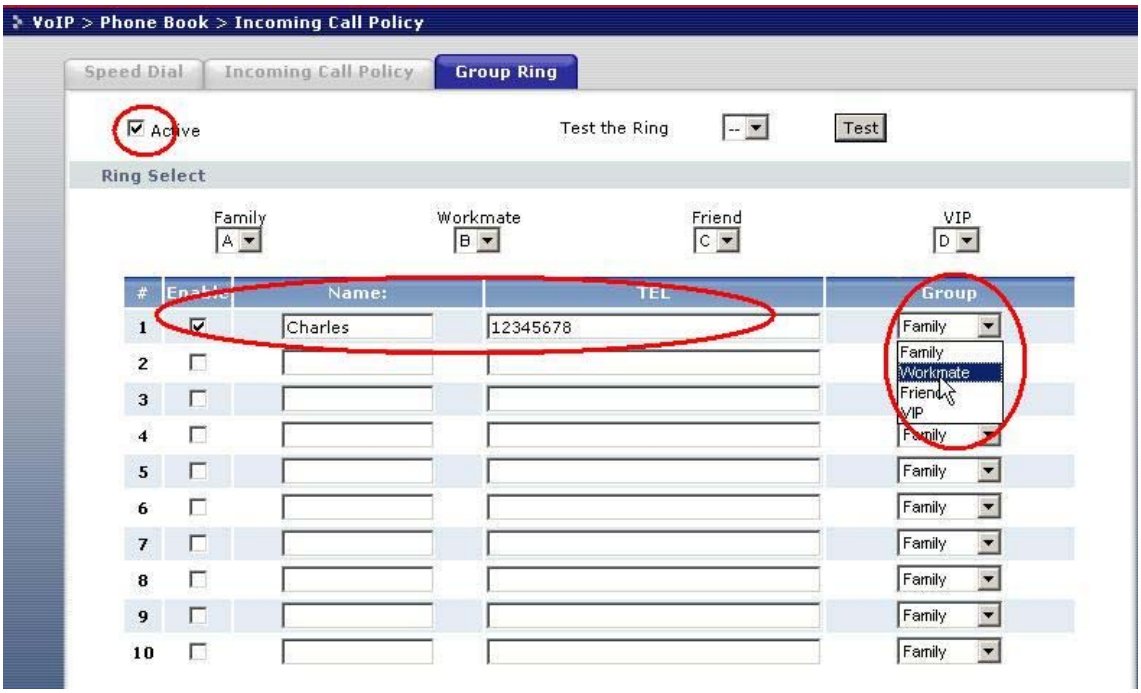
1. Test the ring before configure the group ring function



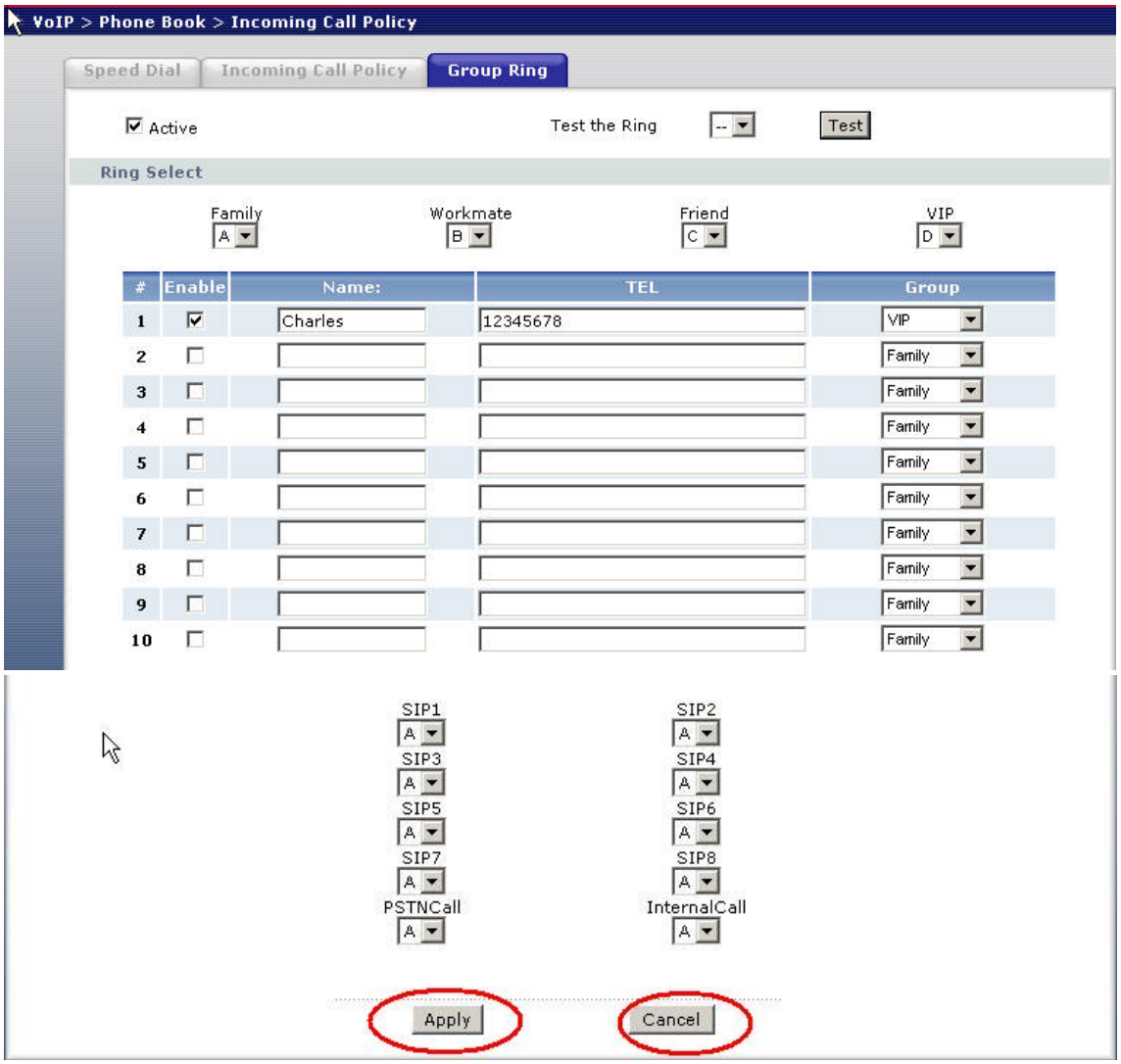
2. Select the ring under each group.(We predefined four different group – Family, Friends, Workmate and VIP). Item "--" means the default ring which differs for each country



3. Fill in the table to configure the group ring. "Name" field means the name of the caller. "TEL" field is the caller's phone number. Then select the distinctive ring by selecting the "Group" item. Finally, mark the "Enable" item to make this entry valid.



4. Save the settings by clicking “Apply” button. If you want to return to the original setting, click on “Reset” button.



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 do I access the embedded web configurator?

The web configurator 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 login password in the Password screen (click SYSTEM > Password). In the Password screen, enter the old password, 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 the 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 need to 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 on the Prestige router to allow more than one person to access the Internet concurrently for the cost of one single user account.

When SUA is enabled on the Prestige and a packet is received from a local client destined for the outside Internet, the Prestige replaces the source address in the IP packet header with its WAN IP 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 is originated from Prestige using the IP address assigned by ISP. When reply packets from the external Internet are received by the Prestige, the original IP source address and TCP/UDP source port numbers are written into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to the intended destination on the LAN. This is because SUA keeps a table of the IP addresses and port numbers currently used by the LAN computers.

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 addresses 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 a 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 rectify the illegal address problem mentioned above without going through each and every host.

The goal of ZyXEL's SUA design 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 up to2048 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 filters or protocol filters?

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

Product FAQ

What is the Prestige Integrated Access Device?

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.

The Prestige series is a robust solution complete with everything you need for providing ADSL Internet access to multiple workstations. The IAD comes with one auto-MDI/MDIX 10/100Mbps Ethernet LAN port and one ADSL WAN port. It is the cost-effective solution that provides easy-to-setup Internet connection for multiple users.

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

Will the Prestige work with my Internet connection?

The Prestige is designed to be compatible with major ISPs offering ADSL broadband service. The Prestige IAD comes with an Ethernet port to connect to your computer so the Prestige is placed between your computer and your ISP. The Prestige also supports PPPoE/PPPoA Internet connection type.

What do I need to use the Prestige?

You need an ADSL modem/router for Internet access over the ADSL line. Prestige is an idea device for such application. The Prestige has one Ethernet port (the LAN port) and one ADSL WAN port. Connect your computer to the LAN port and connect the ADSL line to the WAN port. If you use PPPoE or PPPoA for Internet access, you need to enter the user account information in the Prestige.

What is PPPoE?

PPPoE (**P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet) 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 supports PPPoE since ZyNOS 2.50.

How do I know I am using PPPoE?

PPPoE requires a user account to login to the service provider's server. If you need to enter a user name and password on your computer to connect to the Internet, you are probably using PPPoE. If you connect to the Internet when you turn on your computer, you are probably not using PPPoE. You can check with your ISP or the information sheet given by the ISP. Choose PPPoE as the encapsulation type in the Prestige if your 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 connection. Besides, PPPoE supports a broad range of 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 types does the Prestige have?

The Prestige comes with a 10/100M Ethernet interface to connect to your LAN computer or hub/switch and one 10/100M ADSL interface to the ISP.

What can we do with 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 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 Internet Access Router using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their 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 Internet Access Sharing Router using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their private and secured e-mail, if they have been assigned the proper access rights.

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

Yes. It is possible because Prestige delivers the packet to the local server by looking up a SUA server table. Therefore, to make a local server accessible to the outside users, you must enter the port number and the inside IP address of the server in SMT Menu 15 - SUA Server Setup.

What DHCP capability does the Prestige support?

The Prestige supports DHCP client (Ethernet Encap) 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 addresses to clients on the local LAN.

How to 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 have?

The new Prestige series comes with an auto MDX/MDIX 10/100M Ethernet LAN port to connect to the computer or switch on LAN and one ADSL port for the WAN connection.

How does the Prestige support TFTP?

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

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

註解 [user1]: Is this still true? What about 100/1000 Ethernet?

Cable modems on the same node share the same amount of bandwidth, which means that congestion occurs when too many people 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 (ISPs) today connect to the Internet using a single 1.5 Mbps (or T1) telephone line. All subscribers share that 1.5 Mbps bandwidth. Cable companies connecting to the Internet backbone using a T1 line 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.

What is Multi-NAT?

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

The SUA feature that the Prestige supports previously operates by mapping the private IP addresses to a global IP address. It is a subset of the NAT. The Prestige with ZyNOS V3.00 supports most of the NAT features based on RFC 1631, and we call this feature as **'Multi-NAT'**. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

When do I need Multi-NAT?

a. Make local server accessible from the Internet

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

a. Support Non-NAT Friendly Applications

Some servers providing Internet applications, such as mIRC servers, do not allow users to log in using the same IP address. Thus, users on the same network cannot log into the same server simultaneously. In this case, use the Many-to-Many No Overload or One-to-One NAT mapping types to allow more than one users to access the server from a unique global IP address.

What IP/Port mapping does Multi-NAT support?

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

1. **One-to-One**

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

2. **Many-to-One**

In Many-to-One mode, the Prestige maps multiple ILAs to one IGA. This is equivalent to SUA (also known as PAT, port address translation), ZyXEL's Single User Account (SUA) feature that routers using older ZyNOS versions supported (similar to the SUA-only option on routers with ZyNOS 3.40 or later).

3. **Many-to-Many Overload**

In Many-to-Many Overload mode, the Prestige maps the multiple ILAs to a shared IGA.

4. **Many-to-Many No Overload**

In Many-to-Many No Overload mode, the Prestige maps each ILA to a unique IGA.

5. **Server**

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

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many-to-Many No Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

What is the difference between SUA and Multi-NAT?

SUA (Single User Account) in previous ZyNOS versions is similar to a NAT set with 2 rules (Many-to-One and Server). The Prestige now comes with the Full Feature NAT option to map global IP addresses to local IP addresses for clients or servers. With multiple global IP addresses, multiple severs of the same type (for example, FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions that supported SUA only, you can only set up one server for each service type. On the Prestige, you can apply NAT sets per remote node. They are reusable, but only one set is allowed for each remote node. The Prestige supports two NAT sets since there is only one remote node (the WAN for Internet access). The default SUA (Read-Only) Set in SMT menu 15.1 is a convenient, pre-configured, read-only, Many-to-One mapping set, which is sufficient for most purposes and helpful to people already familiar with SUA in the previous ZyNOS versions.

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 IP or utilize BOOTP/DHCP to request an IP address from the Prestige (the server).

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 accessed from various locations on the Internet. To use this 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.

PSTN Lifeline FAQ

What is P2608 and what is the meaning of L in the model name (for example P2608HWL-D1)?

P2608HW is a SIP-based VoIP/analog telephone adapter. It allows you to send voice signals over the Internet (known as VoIP) using the SIP protocol which is an internationally recognized standard for VoIP technology.

L stands for Lifeline. This Lifeline function is supported in P2608 models with an L in the model name (for example, P2608HWL). P2608HWL supports the PSTN lifeline function. PSTN lifeline allows you to have VoIP and PSTN phone services at the same time.

What is the Lifeline feature?

When power to the Prestige is lost, the Lifeline feature gives you the ability to call specified emergency rescue authority (Police, Fire department etc.) through the P2608HWL as if you are calling on a regular phone.

Do I need Lifeline?

Lifeline support on your VoIP telephone adapter depends on your government regulation or ITSP provider. In some countries, lifeline support is mandatory by law.

Can I connect more than one phone to the phone port?

Yes. P2608HWL Series supports REN (Ringer Equivalence Number) which automatically detects the number of devices connected to the phone line. Your P2608HWL-D1 supports up to three devices per each telephone port.

Can I receive incoming PSTN call through P2608HWL Series?

Yes. P2608HWL Series supports a connection to a PSTNline. This allows you to receive incoming PSTN calls.

Can I make a PSTN call through P2608HWL Series?

Yes. You can make a PSTN call through P2608HWL by pressing a prefix number that you have specified in the web configurator. You can store up to nine prefix numbers on the P2608HWL. In case when power to the P2608HWL is lost, calls are made through the PSTN line; similar to when you make a call using a regular PSTN phone.

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.

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 signals into digital signals and vice versa. There are various speech codecs available 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 one another?

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 trunking 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 using a metric called the Mean Opinion Score (MOS) which is a recommendation by ITU-T. The MOS is a 5-point scale where 5 represents excellent voice quality and 1 represents bad voice quality.

What is codec?

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

What is the relation 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 the Prestige support?

The Prestige supports the following commonly used codecs.

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

Note: G.711 u-law or G.711 a-law is country specific. Thus the Prestige is pre-configured to use the one specific to your country. You can use the CLI to change the codec through Telnet.

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 2608 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 pint 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 keyed in 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 strongly 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 strongly 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.

If you have a firewall in front of the Prestige, make sure that you have configured to firewall to allow SIP pass-through. Make sure the range of RTP ports are also allowed on the firewall.

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

If you can register to 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, this happens when 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).

Firewall FAQ

What is a network firewall?

A firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The firewall can be thought of as two mechanisms: one is to block the traffic, and the other is to permit traffic.

Why is the Prestige firewall secure?

The Prestige firewall is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND attack, IP Spoofing, etc. It also uses stateful packet inspection (SPI) to determine if an inbound connection is allowed through the firewall to the private LAN (behind the Prestige). The Prestige supports Network Address Translation (NAT), which translates the private local addresses to one or multiple public addresses. This adds an additional layer of security since devices on the private LAN are invisible to the Internet.

What are the basic firewall types?

In general, there are three firewall types:

1. Packet Filtering Firewall
2. Application-level Firewall
3. Stateful Inspection Firewall

Packet Filtering Firewalls make forwarding decisions based on the header information in each packet. The header information includes the source, destination addresses and ports of the packet.

Application-level Firewalls are generally hosts running proxy servers which do not allow direct traffic to be transmitted between networks. The proxy servers also perform logging and auditing of traffic passing through them. A proxy server is an application gateway or circuit-level gateway that runs on top of general operating system such as UNIX or Windows NT. It hides valuable data by requiring users to communicate with secure systems by mean of a proxy. A key drawback of application-level firewall is performance.

Stateful Inspection Firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also 'inspect' the session data to assure the integrity of the connection and to adapt to dynamic protocols. The flexible nature of Stateful Inspection firewalls generally provides the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support.

What advantages does the Prestige firewall provide?

1. The Prestige's firewall inspects packet contents and IP headers. It inspects all protocols and understands data in packets intended for other layers (from the network layer to the application layer).
2. The Prestige's firewall performs stateful inspection. It takes into account the state of the connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and be allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
3. The Prestige's firewall uses session filtering, i.e., smart rules, that enhances the filtering process and controls the network session rather than controlling individual packets in a session.
4. The Prestige's firewall is fast. It uses a hashing function to search the matched session cache instead of going through every individual rule for a packet.
5. The Prestige's firewall provides email service to notify you for routine reports and when alerts occur.

Why do you need a firewall when your router has built-in packet filtering and NAT features?

With the increasing growth of Internet usage and online access, companies that do businesses on the Internet face tough security threats. Although packet filtering and NAT restrict access to particular computers and networks, for the other companies this security may be insufficient since packet filtering does not maintain session states. Thus, for greater security, a firewall should be used.

What is a Denial of Service (DoS) attack?

Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

There are four types of DoS attacks:

1. Those that exploits bugs in a TCP/IP implementation such as Ping of Death and Teardrop.

2. Those that exploits weaknesses in the TCP/IP specification such as SYN Flood and LAND Attacks.
3. Brute-force attacks that flood a network with useless data such as Smurf attack.
4. IP Spoofing

What is a Ping of Death attack?

Ping of Death attacks use a 'PING' utility to create an IP packet that exceeds the maximum 65535 bytes of data allowed by the IP specification. The oversized packet is then sent to an unsuspecting system which may crash, hang, or reboot.

What is a Teardrop attack?

Teardrop attacks exploit weakness during the reassembling of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original packet except that it contains an offset field. The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

What is a SYN Flood attack?

SYN attacks flood a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows a SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set a relatively long intervals) terminates the TCP three-way handshake. Once the queue is full , the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

What is a LAND attack?

In a LAN attack, hackers flood SYN packets to the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

What is a Brute-force attack?

A Brute-force attack, such as 'Smurf' attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address of each packet using the broadcast address of the network. Thus the router will

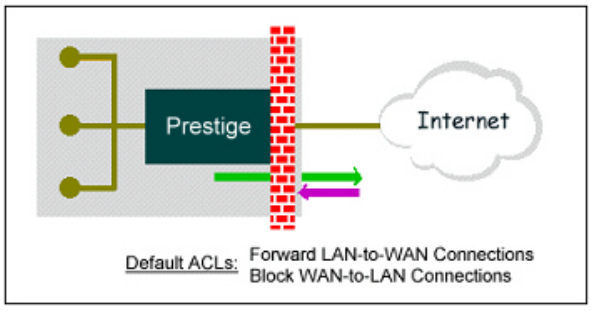
broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request packets, the resulting ICMP traffic will not only clog up the 'intermediary' network, but will also congest the network of the spoofed source IP address, known as the 'victim' network. This flooding of broadcast traffic consumes all available bandwidth, making communications impossible.

What is an IP Spoofing attack?

Many DoS attacks also use IP Spoofing as part of their attack strategy. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP Spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall.

What are the default ACL firewall rules on the Prestige?

There are two default ACLs pre-configured in the Prestige. One allows all connections from the LAN to the WAN and the other blocks all connections from the WAN to the LAN except DHCP packets.



How can I protect against IP spoofing attacks?

The Prestige's firewall will automatically detect the presence of IP spoofing attacks and block suspecting traffic with the firewall turned on. If the firewall is not turned on, you can configure a filter to block IP spoofing attacks. The following shows the basic filter setup.

For the input data filter, set the Prestige to:

- Block packets from the WAN (outside) that claim to be from the LAN (inside)
- Allow everything that is not trying to spoof the Prestige or internal network

Filter rule setup:

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

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

For the output data filters, set the Prestige to:

- Deny bounceback packets
- Allow packets that originated from the Prestige or the internal network hosts

Filter rule setup:

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

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

Content Filter FAQ

What types of content filter does Prestige provide?

Can I have multiple policies enabled at different times of the day or week?

Yes. However, the ZyWALL device currently allows one schedule during which the policies are enabled.

Can I override (block or allow) certain URLs based on a word ?

Yes, You can configure keyword blocking on the ZyXEL device to block access to web sites whose URLs match the specified key words.

How many URL keywords can I configure on the Prestige?

You can configure up to 64 keywords on the Prestige.

IPSec FAQ

What is VPN?

A VPN gives users a secure link to access corporate networks over the Internet or other public or private networks without the expense of lease lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

Why do I need a VPN?

The most common reasons for using a VPN are security and cost.

Security

1). Authentication

With authentication, a VPN device can verify the source of the packets and guarantee data integrity.

2). Encryption

With encryption, a VPN device guarantees the confidentiality of the original user data.

Cost

1). Reduces long distance phone charges

Traditionally, you have to dial to your ISP to establish a VPN connection. Thus using the ZyXEL device as your VPN gateway, you can greatly reduce your phone bills and still enjoy secure VPN connections to remote sites.

2).Reduces the number of access lines required

In the past, most companies pay monthly charges for two types access lines: one high-speed connection for Internet access and one frame relay, ISDN Primary Rate Interface or T1 line to carry data. VPN may allow a company to carry the data traffic over its Internet access lines, thus reducing the need for additional connections for different applications.

What are the most commonly used VPN protocols?

The most commonly used VPN protocols are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec).

What is PPTP?

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

註解 [user2]: Very outdated. What about Windows 2000, XP, Mac OS, or Unix/Linux?

What is L2TP?

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by the Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

What is IPSec?

IPSec is a set of IP extensions developed by IETF (Internet Engineering Task Force) to provide security services compatible with the existing IP standard (IPv.4) and also the upcoming one (IPv.6). In addition, IPSec protects any protocol that runs on top of IP (for instance TCP, UDP, and ICMP). IPSec provides cryptographic security services which enables authentication, integrity, access control, and confidentiality. IPSec allows for the information exchanged between remote sites to be encrypted and verified. You can create encrypted tunnels (VPNs), or just perform encryption between computers. Since you have so many options, IPSec is truly the most extensible and complete network security solution available.

What secure protocols does IPSec support?

There are two protocols provided by IPSec: AH (Authentication Header, protocol number 51) and ESP (Encapsulated Security Payload, protocol number 50).

What are the differences between the 'Transport mode' and 'Tunnel mode'?

The IPSec protocols (AH and ESP) can be used to protect either an entire IP payload or only the upper-layer protocols of an IP payload. Transport mode is mainly for an IP host to protect the data generated locally, while tunnel mode is for a security gateway to provide IPSec service for other machines lacking IPSec capability.

In this case, transport mode only protects the upper-layer protocols of IP payload (user data). Tunnel mode protects the entire IP payload including the user data.

There is no restriction in that the IPSec hosts and the security gateway must be on separate machines. Both IPSec protocols, AH and ESP, can operate in either transport mode or tunnel mode.

What is SA?

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

What is IKE?

IKE is short for Internet Key Exchange. Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration to set up a VPN.

There are two phases in every IKE negotiation- phase 1 (Authentication) and phase 2 (Key Exchange). Phase 1 establishes an IKE SA and phase 2 uses that SA to negotiate SAs for IPSec.

What is a Pre-Shared Key?

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called 'Pre-shared' because you have to share it with another party before you can communicate with them over a secure connection.

What are the differences between IKE and manual key VPN?

The only difference between IKE and manual key is how the encryption keys and SPIs are determined.

- For IKE VPN, the key and SPIs are negotiated from one VPN gateway to the other. After that, the two VPN gateways use this negotiated keys and SPIs to send packets between the two networks.
- For manual key VPN, the encryption key, authentication key (if needed), and SPIs are predetermined by the administrator when configuring the security association.

IKE is more secure than manual key, because IKE negotiation can generate new keys and SPIs randomly for the VPN connection.

What is the use of a Phase 1 ID?

In IKE phase 1 negotiation, the IP address of the remote peer determines which VPN rule must be used to serve the incoming request. However, in some applications, the remote VPN gateway or client software is using an IP address that is dynamically assigned from an ISP, so the Prestige needs additional information to make the decision. Such additional information is what we call phase 1 ID. In IKE payload, there are local and peer ID fields are used for this purpose.

What are Local ID and Peer ID?

Local ID and Peer ID are used in IKE phase 1 negotiation. It’s in FQDN(Fully Qualified Domain Name) format and the IKE standard uses it as a Phase 1 ID type.

Phase 1 ID is an identification for each VPN device on both ends. The type of a Phase 1 ID may be IP, FQDN(DNS) or Users FQDN(E-mail). The content of Phase 1 ID depends on the Phase 1 ID type. The following is an example for how to configure a phase 1 ID.

ID type Content

IP 202.132.154.1
DNS www.zyxel.com
E-mail support@zyxel.com.tw

Please note that in the Prestige, if the "DNS" or "E-mail" type is chosen, you can still enter any character as the content, for example "this_is_Prestige". You don’t have to enter the content in the exact format.

By default, the Prestige and the remote device use IP as the phase 1 ID type. However, if the remote peer uses DNS or E-mail ID type, you must also set the Prestige to use the same ID type.

When should I use FQDN?

If your VPN connection is Prestige-to-Prestige, and both of them have static IP addresses without a NAT router in between, use IP as the Local/Peer ID type.

If either side of VPN tunneling end points uses a dynamic IP address, you may need to configure ID for the VPN gateway with the dynamic IP address. In this case, use "Aggressive mode" for phase 1 negotiation .

Is my Prestige ready for IPSec VPN?

IPSec VPN is available on a Prestige using ZyNOS V3.50 firmware. It is a free upgrade and no registration is required.

By upgrading the firmware and the configuration (romfile) to ZyNOS V3.50, your Prestige is IPSec VPN capable. You can then configure VPN via the web configurator.

Download the firmware from our web site.

NOTE: To update firmware from ZyNOS V3.2x to V3.5x, use the console port or TFTP to perform the firmware upgrade. This is due to the difference in the memory allocation between these two versions.

How do I configure VPN on the Prestige?

You can configure VPN settings on the Prestige using the SMT or Web configurator. Prestige 1 supports Web only.

How many VPN connections does the Prestige support?

Prestige 1 supports 1 VPN connection. Prestige 10 supports 10 VPN connections. Prestige 50 supports 50 tunnels. Prestige 100 supports 100 tunnels.

What VPN protocols are supported on the Prestige?

All Prestige series support ESP (protocol number 50) and AH (protocol number 51).

What VPN encryption types are supported on the Prestige?

The Prestige supports 56-bit DES,168-bit 3DES and AES encryption.

What VPN authentication types does the Prestige support?

VPN vendors support a number of different authentication methods. Prestige VPN supports both SHA1 and MD5.

AH provides authentication, integrity, and replay protection (but not confidentiality). Its main difference with ESP is that AH also secures parts of the packet IP header (like the source/destination addresses), but ESP does not.

ESP provides authentication, integrity, replay protection, and confidentiality of the data (it secures everything in the packet that follows the header). Replay protection requires authentication and integrity (these two always go together). Confidentiality (encryption) can be used with or without authentication/integrity. Similarly, one could use authentication/integrity with or without confidentiality.

I am planning my Prestige-to-Prestige VPN configuration. What do I need to know?

First of all, both Prestiges must have be VPN capable. Check that both are using the V3.50 firmware version or later.

If the VPN feature is available on the Prestige, click **Advanced>VPN** in the web configurator to display the configuration screen.

The following summaries the steps to configure a Prestige-to-Prestige VPN connection.

1. If there is a NAT router running in the front of Prestige, make sure IPSec passthrough is supported and enabled on the NAT router.
2. If NAT is enabled on the network (either in frond of the remote VPN router, or on the Prestige), use the IPSec ESP tunneling mode since NAT does not support the AH mode.
3. **Source IP/Destination IP**—The private IP address ranges of the remote and local networks cannot overlap. VPN will not work if the VPN destination addresses and the local network IP addresses are indistinguishable.
4. **Secure Gateway IP Address** -- This must be a public, routable IP address. A private IP is not allowed. That means it cannot be in the 10.x.x.x, 192.168.x.x, or 172.16.0.0 - 172.31.255.255 range (these address ranges are reserved by the Internet standard for private LANs behind NAT devices). It is usually a static IP so that we can pre-configure it on the Prestige for making VPN connections. If it is a dynamic IP given by your ISP, you can still configure this IP address after the remote Prestige is online and its WAN IP is available from the ISP.

Does the Prestige support dynamic secure gateway IP?

If the remote VPN gateway uses a dynamic IP, enter **0.0.0.0** as the **Secure Gateway IP Address** on the Prestige. In this case, the VPN connection can only be initiated from the gateway that uses the dynamic IP address to the gateway that uses a fixed IP address. This is to allow the gateway with a dynamic IP address to update its dynamic IP address to the remote peer. However, if both gateways use dynamic IP addresses, a VPN connection cannot be established.

Which VPN gateways have been tested to work with the Prestige?

The following VPN gateways have been tested and verified to work with the Prestige.

- Cisco 1720 Router, IOS 12.2(2)XH, IP/ADSL/FW/IDS PLUS IPSEC 3DES
- NetScreen 5, ScreenOS 2.6.0r6
- SonicWALL SOHO 2
- WatchGuard Firebox II
- ZyXEL Prestige 100
- Avaya VPN
- Netopia VPN
- III VPN

Which VPN client software has been tested to work with the Prestige?

The following VPN client software applications have been tested and verified to work with the Prestige.

- SafeNet Soft-PK, 3DES edition
- Checkpoint Software
- SSH Sentinel, 1.4
- SecGo IPSec for Windows
- F-Secure IPSec for Windows
- KAME IPSec for UNIX
- Nortel IPSec for UNIX
- Intel VPN, v. 6.90
- FreeS/WAN for Linux
- SSH Remote ISAKMP Testing Page, (http://isakmp-test.ssh.fi/cgi-bin/nph-isakmp-test)
- Windows 2000, Windows XP IPSec

Will ZyXEL support Secure Remote Management?

Yes. Secure remote management will be available in future firmware releases.

Does the Prestige VPN support NetBIOS broadcast?

NetBIOS broadcasting will be supported in future firmware releases.

Are hosts behind NAT allowed to use IPSec?

NAT Condition	Supported IPSec Protocol
VPN Gateway with NAT enabled	AH tunnel mode, ESP tunnel mode
VPN client/gateway behind NAT*	ESP tunnel mode
NAT in Transport mode	None

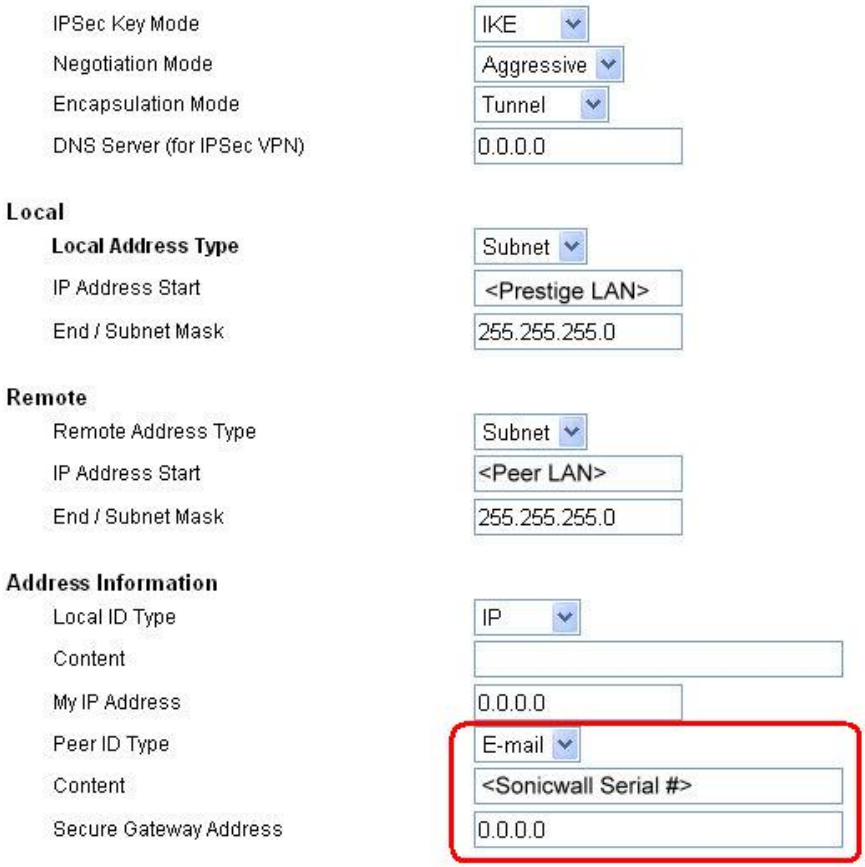
* The NAT router must support IPSec pass through (for example, on Prestige SUA/NAT routers). IPSec pass through is supported on Prestige models using ZyNOS 3.21 firmware or later. The default port and the client IP have to be specified in SMT Menu 15-SUA Server Setup.

Why does VPN throughput decrease when my SMT screen stays at menu 24.1?

If your SMT screen stays at menus 24.1, 24.8 and 27.3, a certain amount of memory is allocated to generate the required statistics. So, it is recommended that you do not leave your SMT screen in menus 24.1, 27.3 and 24.8 when VPN is in use.

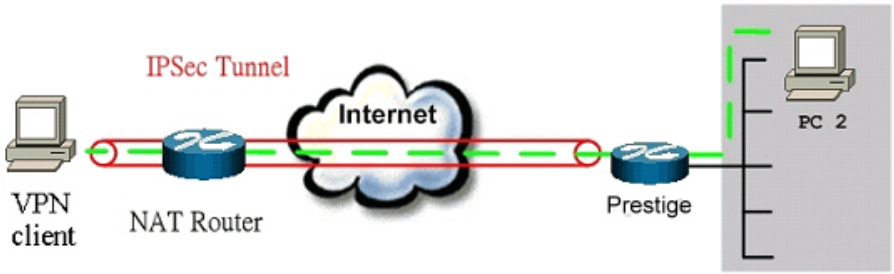
Where can I configure Phase 1 ID on the Prestige?

Phase 1 ID can be configured in the VPN setup screen as follows. Note that you configure the same settings either in the web configurator or SMT.



If I have a NAT router between two VPN gateways, and I would like to use IP type as Phase 1 ID, what information do I need?

The following shows a typical network setup.



VPN client: 10.1.33.33
NAT router WAN IP: 202.132.154.2
Prestige WAN: 202.132.154.3

Since the VPN client is behind a NAT router, it must have a private IP address in most cases. This may cause the VPN client to send its private IP address as the content of its phase 1 ID. So you have to configure the private IP address of the VPN client as the phase 1 ID on the Prestige.

How can I keep a tunnel alive?

To keep a tunnel alive, you can select "**keep alive**" option when configuring your VPN tunnel. With this option, whenever phase 2 SA lifetime is reached, the IKE negotiation procedure will be invoked automatically even without traffic to make the connection stay up.

To reduce consuming system resource, VPN tunnels get disconnected either manually, by a idle timer, or by device shutdown. Packet triggering is still necessary to re-establish the tunnel.

Which IP address types (Single, Range or Subnet) does the Prestige VPN/IPSec support ?

The Prestige supports all IP address types (single, range and subnet). Thus you can specify a single PC, a range of PCs or even a network of PCs to use the VPN/IPSec service.

Does the Prestige support IPSec passthrough?

Yes. The Prestige supports IPSec passthrough. In addition to being a VPN gateway, you can also set the Prestige to work as a NAT router with IPSec passthrough.

If the VPN connection is initiated from a security gateway behind the Prestige, no NAT or Firewall configuration is require.

If the VPN connection is initiated from a security gateway from the remote gateway, you must configure NAT port forwarding and Firewall forwarding on the Prestige.

Configure NAT port forwarding in the web configurator. Click **Setup > "SUA/NAT"** and set the secure gateway's IP address as the default server.

Configure Firewall forwarding in the web configurator. Click **Setup > Firewall**, select **WAN to LAN** Packet Direction and create a firewall rule the forwards IKE(UDP:500) traffic.

Can the Prestige work as a NAT router with IPSec passthrough and an IPSec gateway at

the same time?

No. The Prestige cannot work as a NAT router (with IPSec passthrough) and an IPSec gateway at the same time. You can only set the Prestige work in either one. If the Prestige is to support IPSec passthrough, you have to disable VPN on the Prestige. To disable it, you can either deactivate each VPN rule or use the "ipsec switch off" command in SMT menu 24.8. You can get into the SMT via telnet or the console port.

Wireless FAQ

What is a Wireless LAN ?

Wireless LANs provide all the functionality of wired LANs, without the need for physical connections (wires). Data is modulated onto a radio frequency carrier and transmitted through the air. Typical bit-rates are 11Mbps and 54Mbps, although in practice, data throughput is half of this. Wireless LANs can be formed simply by installing wireless adaptors on the PCs. If connectivity to a wired LAN is required, an Access Point (AP) is used as a bridging device. APs are typically located close to the centre of the wireless network.

What are the advantages of Wireless LANs ?

a. Mobility:
Wireless LAN systems provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.

b. Installation Speed and Simplicity:
Installing a wireless LAN system can be fast and easy and it eliminates the need to pull cables through walls and ceilings.

c. Installation Flexibility:
Wireless technology allows the network to go where wire cannot go.

d. Reduced Cost-of-Ownership:
While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term

cost benefits are greatest in dynamic environments requiring frequent moves and changes.

e. Scalability:

Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

What are the disadvantages of Wireless LANs ?

The speed of Wireless LAN is still relative slower than that of the wired LAN. The most popular wired LAN operates in 100Mbps, which is almost 10 times that of Wireless LANs (10Mbps). A faster wired LAN standard (1000Mbps), which is 100 times faster, has also became popular. The setup cost of Wireless LAN is relative high because the equipment cost including access points and Wireless LAN cards is higher than wired Ethernet devices and CAT 5 cables.

Where can I find wireless 802.11 networks ?

Airports, hotels, and even coffee shops like Starbucks are already using IEEE 802.11 networks so people can wirelessly browse the Internet on their laptops. As these types of networks become more common, this may create additional security risk for remote users if no proper protection is in place.

What is an Access Point ?

An AP (access point also known as a base station) is a wireless device with an antenna and a wired Ethernet connection that broadcasts information using radio signals. APs typically act as a bridge for the clients. They pass information to wireless LAN cards that have been installed in computers or laptops allowing those computers to connect to the campus network or the Internet without wires.

What is IEEE 802.11 ?

IEEE 802.11 is a wireless LAN industry standard, and the objective of IEEE 802.11 is to make sure that different manufactures' wireless LAN devices can communicate to each other. IEEE 802.11 provides 1 or 2 Mbps transmission speeds in the 2.4 GHz ISM band using either FHSS or DSSS.

What is IEEE 802.11b ?

IEEE 802.11b is the first revision of the IEEE 802.11 standard allowing data rates at up to 11Mbps in the 2.4GHz ISM band. Also known as IEEE 802.11 High-Rate or Wi-Fi. 802.11b using only DSSS, the maximum speed of 11Mbps can fall back to 5.5, 2 or 1Mbps.

How fast is IEEE 802.11b ?

The IEEE 802.11b standard has a nominal speed of 11 megabits per second (Mbps). However, depending on signal quality and how many people are using the wireless networks through a particular Access Point, usable speed will be much less (on the order of 4 or 5 Mbps, which is still substantially faster than most dialup, cable and DSL modems).

What is IEEE 802.11a ?

IEEE 802.11a the second revision of IEEE 802.11 that operates in the unlicensed 5 GHz band and allows transmission rates at up to 54Mbps. IEEE 802.11a uses OFDM (orthogonal frequency division multiplexing) as opposed to FHSS or DSSS. Higher data rates are possible by combining channels. Due to higher frequency, range is less than lower frequency systems (i.e., IEEE 802.11b and IEEE 802.11g) and can increase the cost of the overall solution because a greater number of access points may be required. IEEE 802.11a is not directly compatible with IEEE 802.11b or IEEE 802.11g networks. In other words, a user equipped with an IEEE 802.11b or IEEE 802.11g wireless card will not be able to communicate directly to an IEEE 802.11a access point. Instead, you need to use a Multi-mode wireless card.

What is IEEE 802.11g ?

IEEE 802.11g is an extension to IEEE 802.11b. IEEE 802.11g increases the transmission data rates at up to 54 Mbps and still operates in the 2.4 GHz ISM band. Modulation is based on the OFDM (orthogonal frequency division multiplexing) technology. An IEEE 802.11b wireless card can communicate directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower rates depending on the range. The range at 54 Mbps is less than for IEEE 802.11b operating at 11 Mbps.

Is it possible to use products from a variety of vendors ?

Yes. As long as the products comply with the IEEE 802.11 standard. The Wi-Fi logo indicates an IEEE 802.11b compatible product. Wi-Fi5 is a compatibility standard for IEEE 802.11a products operating in the 5GHz band.

What is Wi-Fi ?

The Wi-Fi logo indicates that a product is interoperable with wireless networking equipment from other vendors. A Wi-Fi product has been tested and certified by the Wireless Ethernet Compatibility Alliance (WECA). The Socket Wireless LAN Card is Wi-Fi certified which means that it will work (interoperate) with any brand of Access Points that is also Wi-Fi certified.

What types of devices use the 2.4GHz Band ?

Various spread spectrum radio communication applications use the 2.4 GHz band. This includes WLAN systems (not necessarily of the type IEEE 802.11b), cordless phones, wireless medical telemetry equipment and Bluetooth™ short-range wireless applications, which include connecting printers to computers and connecting modems or hands-free kits to mobile phones.

Does the IEEE 802.11 interfere with Bluetooth devices ?

When multiple devices are operating in the same frequency band, there is a potential for interference.
Both the IEEE 802.11b and Bluetooth devices occupy the same2.4-to-2.483-GHz unlicensed frequency range- thus they operate in the same band. However, a Bluetooth device would not interfere with other IEEE 802.11 devices much more than another IEEE 802.11 device would interfere. While more collisions are possible with the introduction of a Bluetooth device, they are also possible with the introduction of another IEEE 802.11 devices, or any 2.4 GHz cordless phones for that matter. BlueTooth devices are usually low-power, so the effects that a Bluetooth device may have on an IEEE 802.11 network, if any, aren't far-reaching.

Can radio signals pass through walls ?

Transmitting through a wall is possible depending upon the material used in its construction. In general, metals and substances with a high water content do not allow radio waves to pass through. Metals reflect radio waves and concrete attenuates radio waves. The amount of attenuation suffered in passing through concrete will be a function of its thickness and amount of metal re-enforcement used.

What factors may cause interference among WLAN products ?

Factors of interference:

1. Obstacles: walls, ceilings, furniture… etc.
2. Building Materials: metal door, aluminum studs.

3. Electrical devices: microwaves, monitors, electric motors.

Solution :

1.Minimizing the number of walls and ceilings

2.Antenna is positioned for best reception

3.Keep WLAN products away from electrical devices, eg: microwaves, monitors, electric motors,…, etc.

4. Add additional APs if necessary.

What's the difference between a WLAN and a WWAN ?

WLANs are generally privately owned, wireless systems that are deployed in a corporation, warehouse, hospital, or educational campus. Data rates are high and there are no per-packet charges for data transmission.

WWANs are generally publicly shared data networks designed to provide coverage in metropolitan areas and along traffic corridors. WWANs are owned by a service provider or carrier. Data rates are low and charges are based on usage. Specialized applications are characteristically designed around short, burst messaging.

What is Ad Hoc mode ?

A wireless network consists of a number of stations without access points or any connection to a wired network.

What is Infrastructure mode ?

Infrastructure mode implies connectivity to a wired network infrastructure. If such connectivity is required, an Access Points must be used to connect to the wired LAN. Wireless clients must also use "infrastructure mode" in order to access the network through the access points.

How many Access Points are required in a given area ?

This depends on the surrounding terrain, the diameter of the client population, and the number of clients. If an area is large with dispersed pockets of populations, then extension points can be used for extending coverage.

What is the Direct-Sequence Spread Spectrum (DSSS) Technology ?

DSSS spreads its signal continuously over a wide frequency band. DSSS maps the information bearing bit-pattern at the sending station into a higher data rate bit sequence using a "chipping" code. The chipping code (also known as processing gain) introduces redundancy which allows data recovery if certain bit errors occur during transmission. The FCC rules the minimum processing gain should be 10, typical systems use processing gains of 20. IEEE 802.11b specifies the use of DSSS.

What is the Frequency-hopping Spread Spectrum (FHSS) Technology?

FHSS uses a narrowband carrier which hops through a predefined sequence of several frequencies at a specific rate. This avoids problems of fixed channel narrowband noise and simple jamming. Both the transmitter and receiver must have their hopping sequences synchronized to create the effect of a single "logical channel". To unsynchronized receivers, an FHSS transmission appears to be short-duration impulse noise. IEEE 802.11 may use FHSS or DSSS.

Do I need the same kind of antenna on both sides of a link?

No. Provided the antenna is optimally designed for 2.4GHz or 5GHz operation. WLAN NICs often include an internal antenna which may provide sufficient reception.

Why use the 2.4 Ghz Frequency range ?

This frequency range has been set aside by the FCC, and is generally labeled the ISM band. A few years ago Apple and several other large corporations requested that the FCC allow the development of wireless networks within this frequency range. What we have today is a protocol and system that allows for unlicensed use of radio transmissions within a prescribed power level. The ISM band is populated by Industrial, Scientific and Medical devices that are all low power devices, but can interfere with each other.

What is a Server Set ID (SSID) ?

An SSID is a identification name that allows clients to communicate to the appropriate base station. Only clients that are configured to use the same SSID can communicate with the base stations having the same SSID. From a security point of view, SSID provides a simple single shared password between the base stations and clients.

What is an ESSID ?

ESSID stands for Extended Service Set Identifier and it identifies the wireless LAN. The ESSID of a mobile device must match the ESSID of the AP to communicate with the AP. The ESSID is a 32-character

string and is case-sensitive.

How do I secure data transmitted to/from an Access Point over the wireless connection?

Enable Wired Equivalency Protocol (WEP) or Wi-Fi Protected Access (WPA) to encrypt the payload of the packets sent across a wireless connection.

What is WEP?

Wired Equivalent Privacy (WEP) is a security mechanism defined in the IEEE 802.11 standard and is designed to ensure that the security of the wireless medium equal to that of a cable (wire). WEP data encryption is designed to prevent access to the network from unauthorized users or "intruders" and to prevent wireless LAN traffic from been eavesdropped. WEP allows administrators to define a set of security "Keys" for each wireless user based on a "Key String" based on the WEP encryption algorithm. Access is denied from anyone who does not have an assigned key. You can configure 40/64-bit and 128-bit encryption key lengths for WEP. However, WEP is known to have flaws in its key generation processing.

What is the difference between 40-bit and 64-bit WEP keys?

40-bit WEP and 64-bit WEP have the same encryption level, thus they are essentially the same. WEP encryption uses 40 bits (10 Hex character) for the "secret key" (set by the user), and a 24-bit " Initialization Vector " (not under user control) (40+24=64). Some vendors refer this level of WEP as 40-bit, while others refer it as 64-bit WEP.

What is a WEP key ?

A WEP key is a user-defined string of characters used to encrypt and decrypt data.

A WEP key is a user-defined string of characters used to encrypt and decrypt data?

Wireless clients must use the same WEP key and the same key length to communicate with one another. This means that a wireless client using a 128-bit WEP key cannot communicate with a peer wireless client who is using a 64-bit or 256-bit WEP. Although a 128-bit WEP key also uses a 24-bit Initialization Vector, it uses a 104-bit secret key.

Can the SSID be encrypted?

WEP, the encryption standard for IEEE 802.11, only encrypts data packets not IEEE 802.11 management packets and the SSID is in the beacon and probe management messages. Thus, an SSID is not encrypted if WEP is turned on. An SSID is transmitted in clear text in the wireless network. This makes obtaining an SSID easy by sniffing any IEEE 802.11 wireless traffic.

By turning off SSID broadcasting, can someone still sniff the SSID?

By default, many APs broadcast their SSIDs. Sniffers can easily scan and obtain the SSIDs in broadcast beacon packets. Turning off SSID broadcasting in the beacon message (a common practice) does not prevent anyone from obtaining or scanning the SSID. Since an SSID is sent in the clear in the probe message when a wireless client associates to an AP, a snifter just has to wait for a valid user to associate to the network to see the SSID.

What are Insertion Attacks?

Insertion attacks allow an intruder to access a network by placing unauthorized devices on the wireless network without going through the security process (such as authentication).

What is a Wireless Snifter?

An attacker can sniff and capture legitimate traffic. Most Ethernet snifter tools capture the first part of the connection session, where information such as the username and password are included. An intruder can masquerade as a legitimate user by using the account information obtained. An intruder who monitors the wireless traffic can apply this same method to gain access to the wireless network.

What is the difference between Open System and Shared Key Authentication Types ?

Open System:
This is the default authentication service that simply announces the desire to associate with another station or access point. A station can authenticate with any other station or access point using open system authentication if the receiving station also uses open system authentication.

Share Key:
This is the optional authentication method that involves a more rigorous exchange of frames, ensuring that the requesting station is authentic. For a station to use shared key authentication, it must implement

WEP.

What is the difference between No authentication required, No access allowed and Authentication required?

No authentication required—disables IEEE 802.1X and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without IEEE 802.1X-based authentication of the client.
No access allowed—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.
Authentication required—enables IEEE 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The device requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the device by the client's MAC address.

What is AAA?

AAA (Authentication, Authorization, and Accounting) refers to the idea of managing subscribers by controlling their access to the network, verifying that they are who they say they are (via login names and passwords or MAC addresses) and accounting for their network usage.

What is RADIUS?

RADIUS (Remote Authentication Dial-In User Service) is a standard that has been implemented into several software packages and networking devices. It allows user information to be sent to a central database running on a RADIUS Server, where it is verified. RADIUS also provides a mechanism for accounting.

What is WPA?

WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i security specification draft. Key difference between WPA and WEP are user authentication and improve data encryption.

What is WPA-PSK?

WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) can be used if user do not have a RADIUS server but still want to benefit from it. Because WPA-PSK only requires a single password to be entered on the wireless AP/gateway and the wireless client. As long as the passwords match, a client will be granted access to the WLAN.

Troubleshooting

For general device installation or basic troubleshooting, refer to the device user's guide

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**
1.5 Display the 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**
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 make system to enter the debug 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 01 ed 2b ...b...f...j...n
e5bdc020: 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 01 ed 2b ...b...f...j...n
e5bdc040: 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 01 ed 2b ...b...f...j...n
e5bdc060: 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 01 ed 2b ...b...f...j...n
e5bdc080: 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 01 ed 2b ...b...f...j...n
e5bdc0a0: 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 01 ed 2b ...b...f...j...n
e5bdc0c0: 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 01 ed 2b ...b...f...j...n
e5bdc0e0: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
Bootbase Version: V1.10 | 12/02/2004 14:00:00
RAM: Size = 16384 Kbytes
FLASH: Intel 16M *1

ZyNOS Version: V3.40(RE.0) | 01/27/2005  15:00:00
Enter Debug Mode
atgo
    (Compressed)
    Version: RAS P2608HWL, start: bfc58030
    Length: 3DB3EC, Checksum: 9AA9
    Compressed Length: 12AC58, Checksum: DC06

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
initialize ch = 0, ethernet address: 00:a0:c5:d1:78:e9
Wan Channel init ........ done
..................................... done
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 the real-time trace results on 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 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 Display brief online trace results online : `sys trcd brief`
or
1.5 Display detailed online trace results online : `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    11883.2608HWL ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  10    11883.2608HWL 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 (2608HWL40)
    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 (2608HWL40)
  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 the 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.