

# Prestige 2602HWL-DXA

## Support Notes

Version 3.40

Feb. 2006



**Index**

<b>Application Notes .....</b>	<b>9</b>
General Application Notes .....	9
Internet Connection.....	9
Setup the Prestige as a DHCP Relay.....	13
Configure an Internal Server Behind SUA .....	15
Configure a PPTP server Behind SUA .....	17
Using NAT / Multi-NAT .....	21
About Filter & Filter Examples .....	42
Using the Dynamic DNS (DDNS).....	65
Network Management Using SNMP .....	67
Using syslog.....	73
Using IP Alias .....	77
Using Call Scheduling .....	79
Using IP Multicast .....	84
Using Prestige traffic redirect .....	86
Using Universal Plug n Play (UPnP).....	88
Wireless Application Notes.....	94
Infrastructure mode .....	94
Wireless MAC address filtering.....	99
WEP configuration (Wired Equivalent Privacy).....	102
Configuring 802.1x .....	109
Site Survey .....	122
PSTN Lifeline Application Notes .....	125
Usage of PSTN Lifeline.....	125
Lifeline configuration .....	126
Relay to PSTN .....	127
How to connect Lifeline and DSL connection.....	127
VoIP Application Notes.....	128
Setup SIP Account .....	129
Peer to Peer call .....	132
Phone port settings .....	136
Advanced voice settings configuration.....	138
Phone book Speed dial.....	141
Voice - QoS setup .....	144
Call Forwarding setup.....	145

Voice – Common Settings .....	148
<b>FAQ .....</b>	<b>149</b>
ZyNOS FAQ .....	149
What is ZyNOS? .....	149
How do I access the embedded web configurator?.....	150
What is the default LAN IP address and Password? Moreover, how do I change it? .....	150
How do I upload the ZyNOS firmware code via embeded web configurator? .....	150
How do I upgrade/backup the ZyNOS firmware by using FTP client program via LAN? .....	150
How do I upload or backup ROMFILE via web configurator?.....	151
How do I backup/restore configurations by using FTP client program via LAN?.....	151
Why can't I make Telnet to Prestige from WAN? .....	152
What should I do if I forget the system password?.....	152
What is SUA? When should I use SUA?.....	152
What is the difference between NAT and SUA?.....	153
How many network users can the SUA/NAT support?.....	153
What are Device filters and Protocol filters?.....	153
Why can't I configure device filters or protocol filters? .....	153
Product FAQ .....	154
What is the Prestige Integrated Access Device? .....	154
Will the Prestige work with my Internet connection?.....	154
What do I need to use the Prestige? .....	154
What is PPPoE? .....	154
Does the Prestige support PPPoE?.....	155
How do I know I am using PPPoE?.....	155
Why does my provider use PPPoE?.....	155
Which Internet Applications can I use with the Prestige? .....	155
How can I configure the Prestige? .....	155
What network interface does the Prestige support?.....	155
What can we do with Prestige? .....	155
Does Prestige support dynamic IP addressing? .....	156
What is the difference between the internal IP and the real IP from my ISP? .....	156
How does e-mail work through the Prestige? .....	156

Is it possible to access a server running behind SUA from the outside Internet? If possible, how? .....	156
What DHCP capability does the Prestige support?.....	156
How do I used the reset button, more over what field of parameter will be reset by reset button? .....	157
What network interface does the new Prestige series support? .....	157
How does the Prestige support TFTP?.....	157
Can the Prestige support TFTP over WAN? .....	157
How fast can the data go? .....	157
What is Multi-NAT? .....	158
When do I need Multi-NAT? .....	158
What IP/Port mapping does Multi-NAT support? .....	159
What is the difference between SUA and Multi-NAT? .....	160
What is BOOTP/DHCP?.....	160
What is DDNS?.....	161
When do I need DDNS service? .....	161
What DDNS servers does the Prestige support?.....	161
What is DDNS wildcard?.....	161
Does the Prestige support DDNS wildcard?.....	161
Can the Prestige SUA handle IPsec packets sent by the VPN gateway behind Prestige? .....	162
How do I setup my Prestige for routing IPsec packets over SUA? .....	162
PSTN Lifeline FAQ .....	162
What is P2602 and what is the difference between P2602HW and P2602HWL? .....	162
What does Lifeline mean? .....	162
Do I need Lifeline? .....	162
Can I connect more than one phone on the phone port?.....	163
Can I receive incoming PSTN call through P2602HWL- 6xC? .....	163
Can I make an outgoing PSTN call through P2602HWL – 6xC? .....	163
VoIP FAQ .....	163
What is Voice over IP? .....	163
How does Voice over IP work? .....	163
Why use VoIP? .....	163
What is the relationship between codec and VoIP?.....	164
What advantage does Voice over IP can provide?.....	164
What is the difference between H.323 and SIP?.....	164

Can H.323 and SIP interoperate with one another?.....	164
What is voice quality?.....	164
How are voice quality normally rated?.....	164
What is codec? .....	165
What is the relation of codec and VoIP? .....	165
What codec does Prestige support?.....	165
Which codec should I choose?.....	165
What do I need in order to use SIP? .....	165
Unable to register with the SIP server?.....	166
I can register but can not establish a call?.....	166
I can make a call but the voice only goes one way not bothway? .....	166
I can receive a call but the voice only goes one way not bothway? .....	166
If all the about have been tried, but register still fail what should I do?....	167
I suspect there is a hardware problem with my Prestige what should I do?167	
Firewall FAQ .....	167
What is a network firewall? .....	167
What makes Prestige firewall secure? .....	167
What are the basic types of firewalls? .....	168
What kind of firewall is the Prestige?.....	168
Why do you need a firewall when your router has packet filtering and NAT built-in?.....	169
What is Denials of Service (DoS)attack?.....	169
What is Ping of Death attack?.....	169
What is Teardrop attack? .....	169
What is SYN Flood attack?.....	169
What is LAND attack?.....	170
What is Brute-force attack? .....	170
What is IP Spoofing attack?.....	170
What are the default ACL firewall rules in Prestige? .....	170
How can I protect against IP spoofing attacks?.....	171
Content Filter FAQ .....	172
IPSec FAQ .....	172
What is VPN? .....	172
Why do I need VPN? .....	173
What are most common VPN protocols?.....	173
What is PPTP? .....	173
What is L2TP? .....	174

What is IPSec? .....	174
What secure protocols does IPSec support? .....	174
What are the differences between 'Transport mode' and 'Tunnel mode'?... ..	174
What is SA? .....	175
What is IKE?.....	175
What is Pre-Shared Key? .....	175
What are the differences between IKE and manual key VPN? .....	175
What is Phase 1 ID for? .....	175
What are Local ID and Peer ID?.....	176
When should I use FQDN? .....	176
Is my Prestige ready for IPSec VPN? .....	176
How do I configure Prestige VPN? .....	177
How many VPN connections does Prestige support?.....	177
What VPN protocols are supported by Prestige?.....	177
What types of encryption does Prestige VPN support? .....	177
What types of authentication does Prestige VPN support? .....	177
I am planning my Prestige-to-Prestige VPN configuration. What do I need to know?.....	177
Does Prestige support dynamic secure gateway IP?.....	178
What VPN gateway that has been tested with Prestige successfully? .....	178
What VPN software that has been tested with Prestige successfully?.....	179
Will ZyXEL support Secure Remote Management?.....	179
Does Prestige VPN support NetBIOS broadcast? .....	179
Is the host behind NAT allowed to use IPSec? .....	179
Why does VPN throughput decrease when staying in SMT menu 24.1?..	179
Where can I configure Phase 1 ID in Prestige? .....	180
If I have NAT router between two VPN gateways, and I would like to use IP type as Phase 1 ID, what should I know? .....	180
How can I keep a tunnel alive? .....	181
Single, Range, Subnet, which types of IP address do Prestige 10/10II/10W/50/100 support in VPN/IPSec? .....	181
Can Prestige support IPSec passthrough?.....	181
Can Prestige behave as a NAT router supporting IPSec passthrough and an IPSec gateway simultaneously?.....	182
Wireless FAQ .....	182
What is a Wireless LAN ? .....	182
What are the advantages of Wireless LANs ? .....	182

What are the disadvantages of Wireless LANs ?.....	183
Where can you find wireless 802.11 networks ? .....	183
What is an Access Point ?.....	183
What is IEEE 802.11 ?.....	184
What is 802.11b ? .....	184
How fast is 802.11b ?.....	184
What is 802.11a ?.....	184
What is 802.11g ? .....	184
Is it possible to use products from a variety of vendors ?.....	185
What is Wi-Fi ?.....	185
What types of devices use the 2.4GHz Band ? .....	185
Does the 802.11 interfere with Bluetooth devices ? .....	185
Can radio signals pass through walls ? .....	185
What are potential factors that may causes interference among WLAN products ?.....	186
What's the difference between a WLAN and a WWAN ?.....	186
What is Ad Hoc mode ? .....	186
What is Infrastructure mode ?.....	186
How many Access Points are required in a given area ? .....	187
What is Direct-Sequence Spread Spectrum Technology – (DSSS) ?.....	187
What is Frequency-hopping Spread Spectrum Technology – (FHSS) ? ...	187
Do I need the same kind of antenna on both sides of a link ?.....	187
Why the 2.4 Ghz Frequency range ?.....	187
What is Server Set ID (SSID) ? .....	187
What is an ESSID ?.....	188
How do I secure the data across an Access Point's radio link ?.....	188
What is WEP ? .....	188
What is the difference between 40-bit and 64-bit WEP ?.....	188
What is a WEP key ? .....	188
A WEP key is a user defined string of characters used to encrypt and decrypt data ? .....	189
Can the SSID be encrypted ? .....	189
By turning off the broadcast of SSID, can someone still sniff the SSID ?	189
What are Insertion Attacks ?.....	189
What is Wireless Sniffer ? .....	189
What is the difference between Open System and Shared Key of Authentication Type ?.....	189

What is 802.1x ? .....	190
What is the difference between No authentication required, No access allowed and Authentication required ? .....	190
What is AAA ?.....	190
What is RADIUS ?.....	190
What is WPA ?.....	191
What is WPA-PSK?.....	191
<b>Trouble Shooting .....</b>	<b>191</b>
Using Embedded Packet Trace .....	191
Debug PPPoE Connection .....	206
<b>CLI Command List .....</b>	<b>218</b>



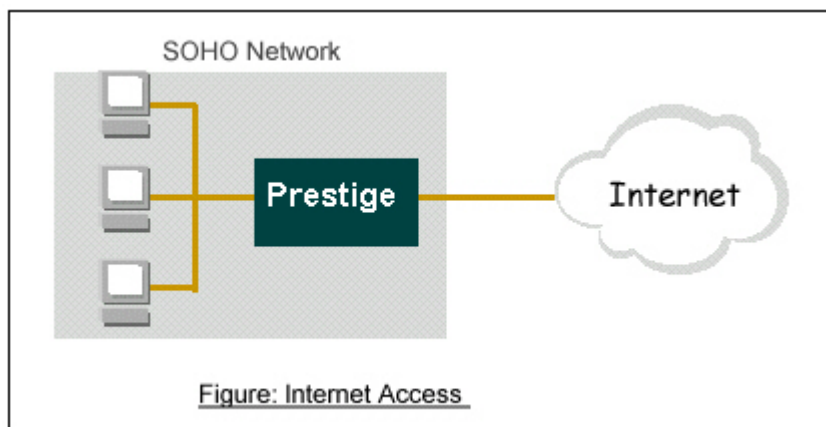
## Application Notes

### General Application Notes

#### Internet Connection

A typical Internet access application of the Prestige is shown below. For a small office, there are some components needs to be checked before accessing the Internet.

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



- 
- Before you begin

The Prestige is shipped with the following factory default:

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

- Setting up the PC (Windows OS)

#### 1. Ethernet connection

All PCs must have an Ethernet adapter card installed.

- If you only have one PC, connect the PC's Ethernet adapter to the Prestige's LAN port with a crossover (red one) Ethernet cable.
- If you have more than one PC, both the PC's Ethernet adapters and the Prestige's LAN port must be connected to an external hub with straight Ethernet cable.

## 2. TCP/IP Installation

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

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

Note: Do not assign arbitrary IP address and subnet mask to your PCs, 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 PC. Make sure your Prestige is powered on before answering Yes to the prompt. Repeat the above steps for each Windows PC on your network.
- **Setting up the Prestige router**

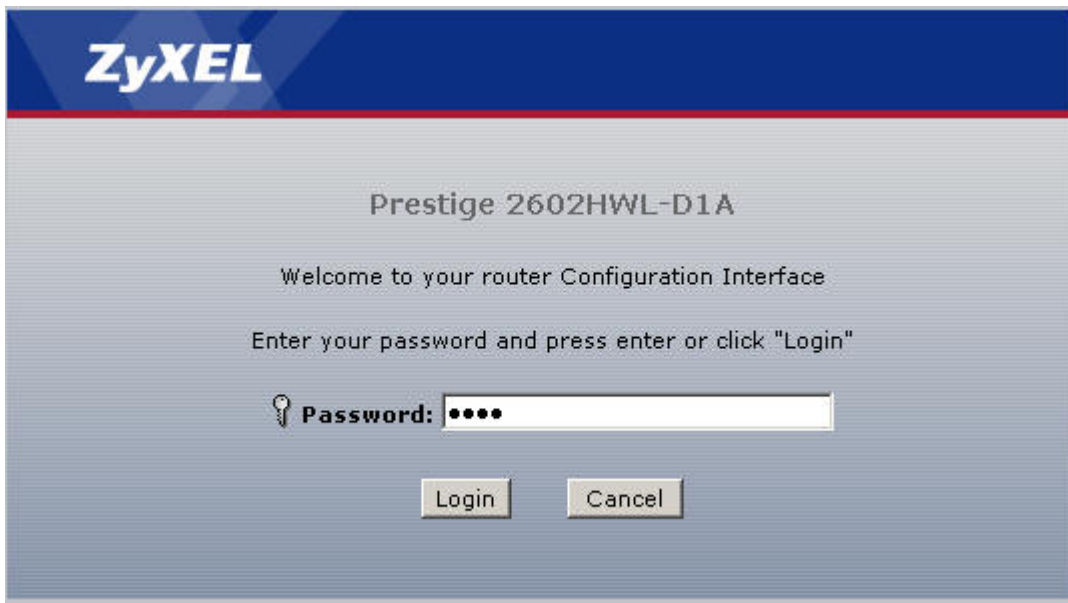
The following procedure is for the most typical usage of the Prestige where you have a single-user account (SUA). The Prestige supports embedded web server that allows you to use Web browser to configure it. Before configuring the router using Browser please be sure there is no Telnet or Console login.

### 1. Retrieve Prestige Web

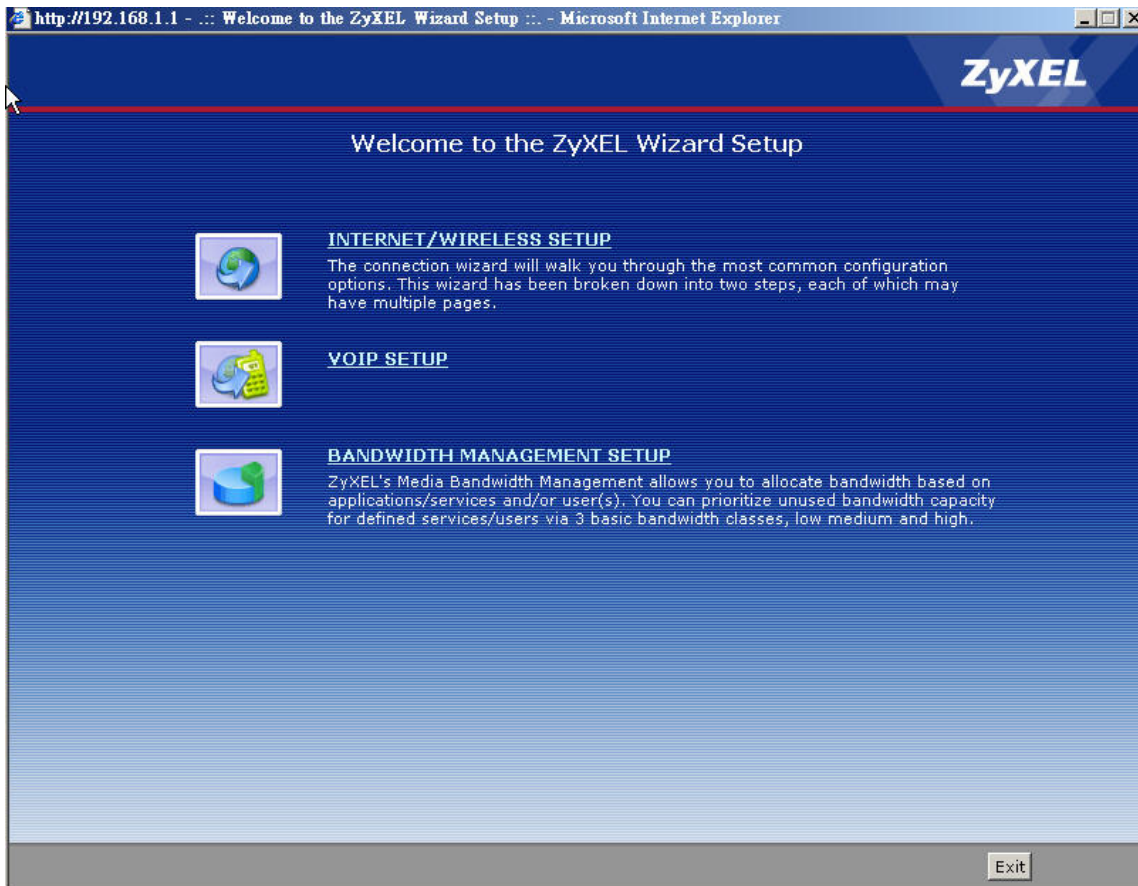
Please enter the LAN IP address of the Prestige router in the URL location to retrieve the web screen from the Prestige. The default LAN IP of the Prestige is 192.168.1.1. See the example below. Note that you can either use <http://192.168.1.1>

### 2. Login first

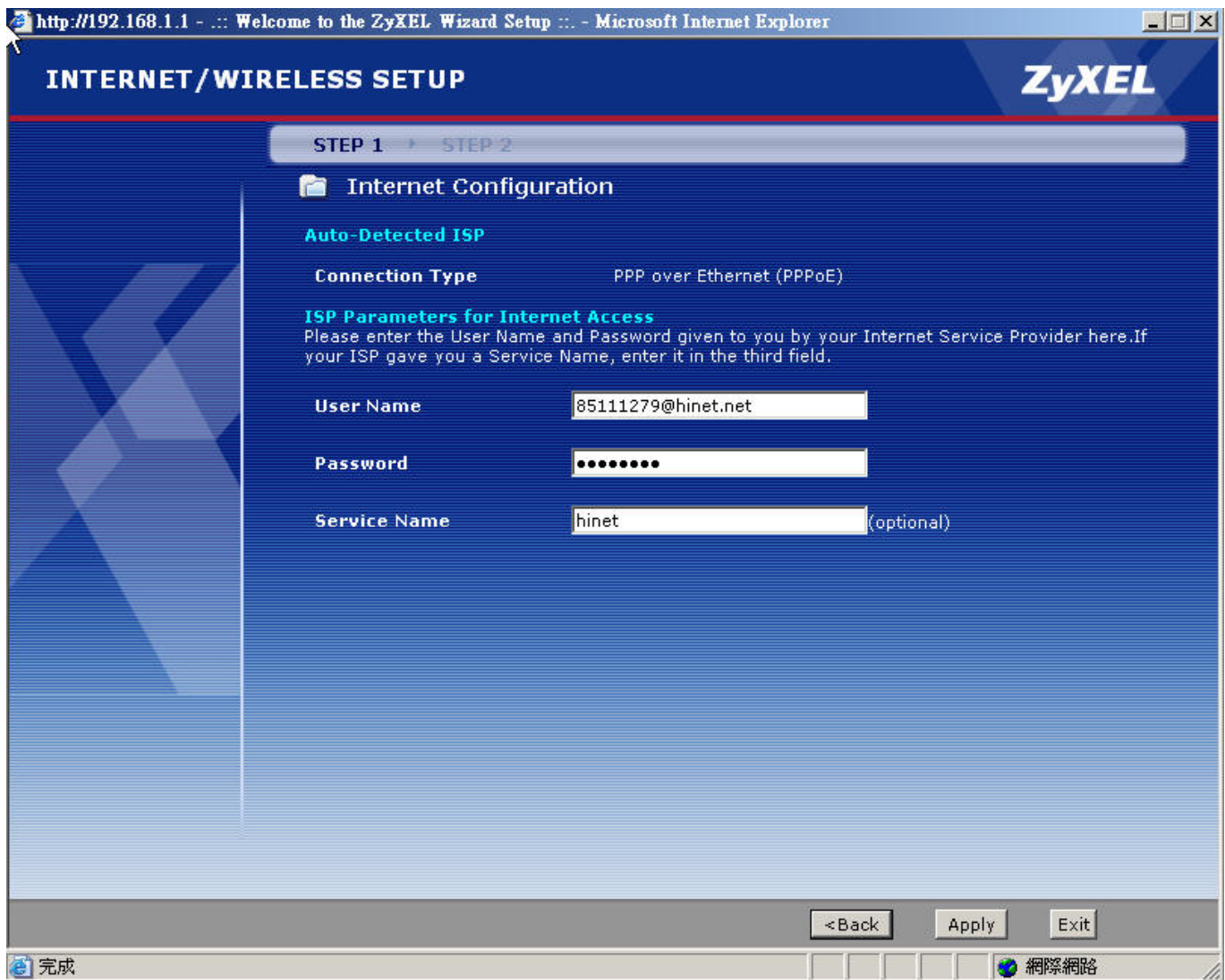
The default password is the default SMT password, '1234'.



### 3. Configure Prestige for Internet access by using **WIZARD SETUP**



The Web screen shown below takes PPPoE as the example.

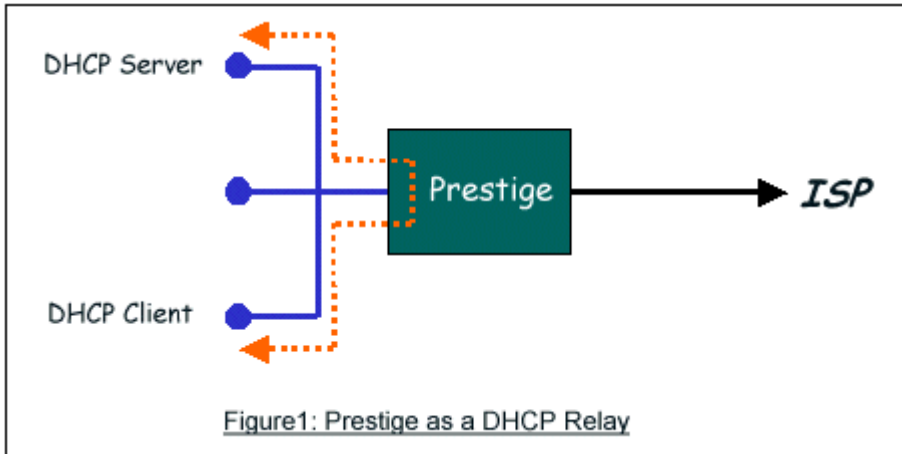


## Setup the Prestige as a DHCP Relay

- What is DHCP Relay?

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P2602 supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the

LAN clients. When it is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 1.



- Setup the Prestige as a DHCP Client

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

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

##### DHCP Setup

DHCP= **Relay**

Client IP Pool Starting Address= N/A

Size of Client IP Pool= N/A

Primary DNS Server= N/A

Secondary DNS Server= N/A

Remote DHCP Server= **192.168.1.2**

##### TCP/IP Setup:

IP Address= 192.168.1.1

IP Subnet Mask= 255.255.255.0

RIP Direction= None

Version= N/A

Multicast= None

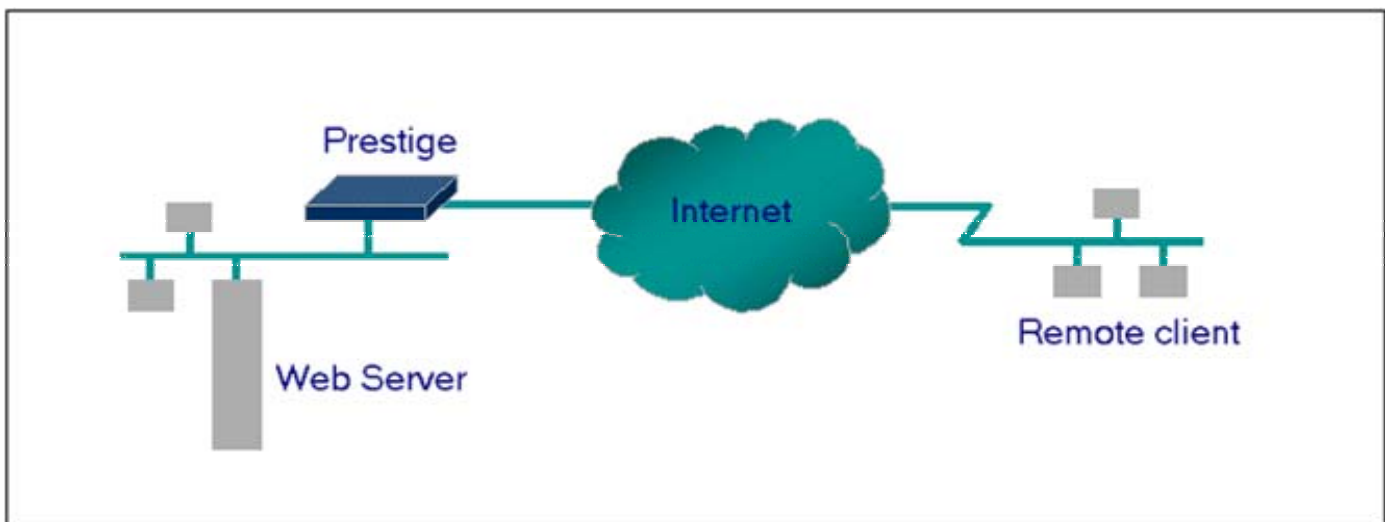
IP Policies=

Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

---

### Configure an Internal Server Behind SUA



- Introduction

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

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

---

- Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server in 'Menu 15.2.1', Multiple Server Configuration. The outside users can access the local server using the Prestige's *WANIP* address which can be obtained from menu 24.1.

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

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:

- Port numbers for some services

Service	Port Number
FTP	21
Telnet	23
SMTP	25



DNS (Domain Name Server)	53
www-http (Web)	80

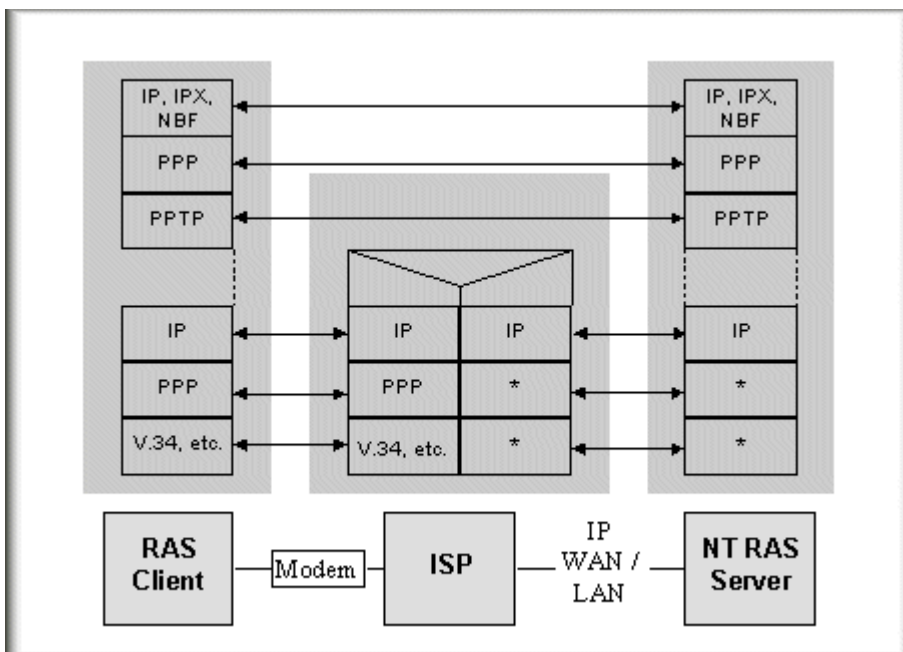
**Configure a PPTP server Behind SUA**

- Introduction

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

In order to run the Windows 9x PPTP client, you must be able to establish an IP connection with a tunnel server such as the Windows NT Server 4.0 Remote Access Server.

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



Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

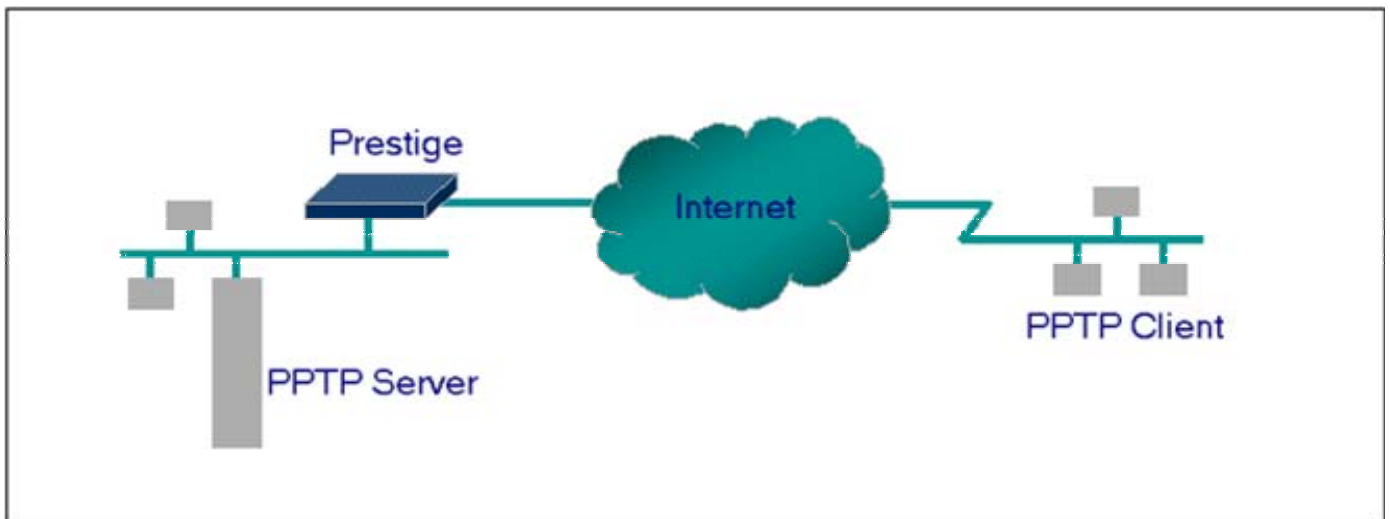
PPTP appears as new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the Dial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system.

Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial-up adapter that provides PPP support for the analog or ISDN modem.

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

- **Configuration**

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



- **Example**

The following example shows how to dial to an ISP via the Prestige and then establish a tunnel to a private network. There will be three items that you need to set up for PPTP application, these are PPTP server (WinNT), PPTP client (Win9x) and the Prestige.

- **PPTP server setup (WinNT)**
  - Add the VPN service from Control Panel>Network
  - Add an user account for PPTP logged on user
  - Enable RAS port
  - Select the network protocols from RAS such as IPX, TCP/IP NetBEUI
  - Set the Internet gateway to Prestige

- PPTP client setup (Win9x)
  - Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the Prestige's Internet IP address for logging to NT RAS server.
  - Set the Internet gateway to the router that is connecting to ISP
  
- Prestige router setup
  
- Before making a VPN connection from Win9x to WinNT server, you need to connect Prestige router to your ISP first.
- Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown 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
<b>2.</b>	<b>1723</b>	<b>1723</b>	<b>192.168.1.10</b>
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the

Internet. If the Internet connection between two LANs is achieved, you can place a VPN call from the remote Win9x client.

For example:

```
C:\ping 203.66.113.2
```

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

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

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



## Using NAT / Multi-NAT

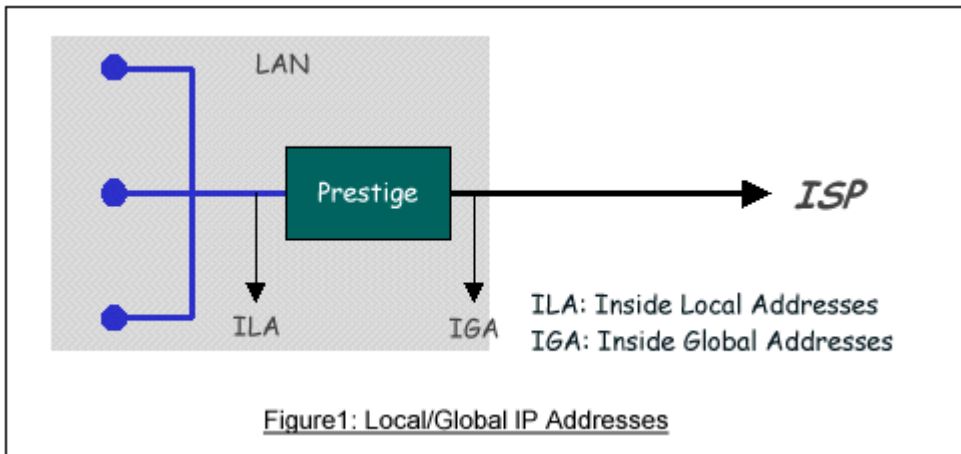
- What is Multi-NAT?

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. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the 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 only one subset of the NAT. The Prestige with Zynos V3.40 supports the most of the features of the NAT based on RFC 1631, and we call this feature as **'Multi-NAT'**. For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

- How NAT works

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



### 1. NAT Mapping Types

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

#### 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 ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

#### 4. **Many to Many Overload**

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

#### 5. **Many to Many No Overload**

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

- **Server**

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

The following table summarizes these types.

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

- **SUA Versus NAT**

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. The Prestige now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple servers of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions (that supported SUA 'visible' servers had to be of different types. The Prestige supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The Prestige 2602HWL supports 8 sets since there are 8 remote node. The default SUA (Read Only) Set in menu 15.1 is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions.

- **SMT Menus**

**1. Applying NAT in the SMT Menus**

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

```

Menu 4 - Internet Access Setup

ISP's Name= 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= Full Feature
    Address Mapping Set= 1

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the options for Network Address Translation.

Field	Options	Description
Network Address Translation	<b>Full Feature</b>	When you select this option the SMT will use Address Mapping Set 1 (Menu 15.1-see later for further discussion).
	<b>None</b>	NAT is disabled when you select this option.
	<b>SUA Only</b>	When you select this option the SMT will use Address Mapping Set 255 (Menu 15.1-see later for further discussion). This option use basically Many-to-One

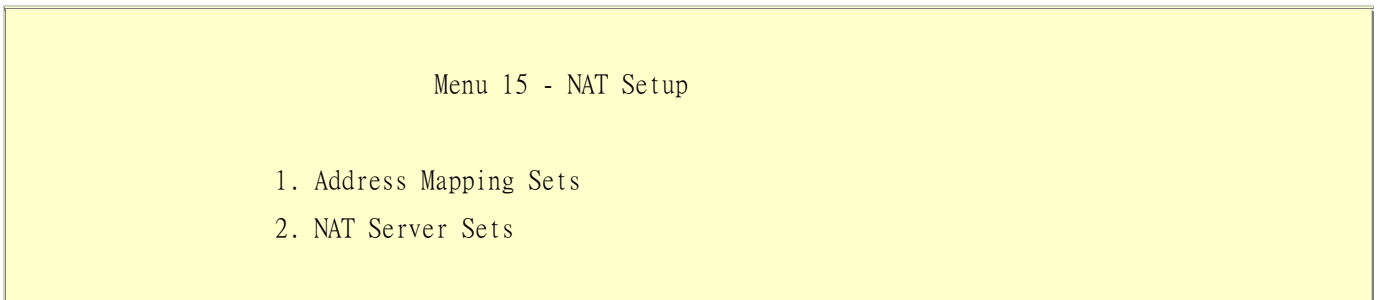


	Overload mapping. Select <b>Full Feature</b> when you require other mapping types. It is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous Zynos versions. Note that there is also a <b>Server</b> type whose IGA is <b>0.0.0.0</b> in this set.
--	---

Table: Applying NAT in Menu 4 and Menu 11.3

## 2. Configuring NAT

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

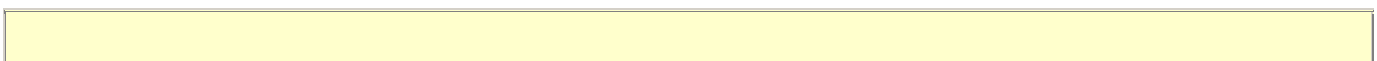


## 3. Address Mapping Sets and NAT Server Sets

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to LAN clients. Each remote node must specify which NAT Address Mapping Set to use. The P2602HWL has 8 remote nodes and so allows you to configure 8 NAT Address Mapping Set. You can see nine NAT Address Mapping sets in Menu 15.1. You can only configure from Set 1 to Set 8. Set 255 is used for SUA. When you select **Full Feature** in menu 4 or 11.3. When you select **SUA Only**, the SMT will use Set 15.2.

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

Enter 1 to bring up Menu 15.1-Address Mapping Sets



Menu 15.1 - Address Mapping Sets

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 255. SUA (read only)

Enter Set Number to Edit:

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

Menu 15.1.1 - 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 fields in this screen. Please note that the fields in this menu are read-only.

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

Please note that the fields in this menu are read-only. However, the settings of the server set 1 can be modified in menu 15.1.1.

Now let's look at Option 1 in Menu 15.1.1 Enter 1 to bring up this menu.

```

Menu 15.1.1 - Address Mapping Rules
Set Name= ?
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.
2.
3.
4.
5.
6.
7.
8.
    
```

9.  
10.

Action= Edit                      , Select Rule= 0

Press ENTER to Confirm or ESC to Cancel:

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

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

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

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

Menu 15.1.1.1 - - Rule 1

Type: One-to-One

```

Local IP:
  Start= 0.0.0.0
  End  = N/A
Global IP:
  Start= 0.0.0.0
  End  = N/A

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

The following table describes the fields in this screen.

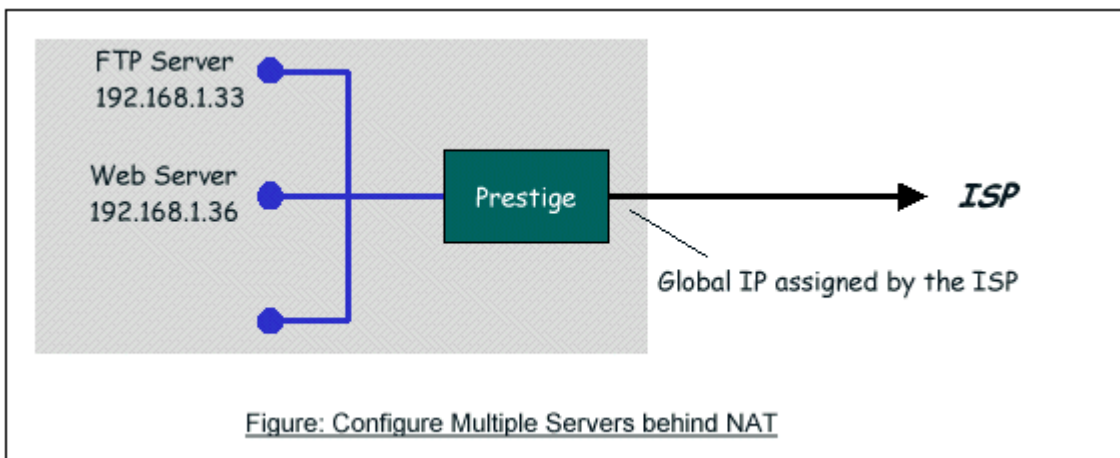
Field		Description	Option/Example
Type		Press [SPACEBAR] to toggle through a total of 5 types. These are the mapping types discussed above plus a server type. Some examples follow to clarify these a little more.	One-to-One Many-to-One Many-to-Many Overload Many-to-Many No Overload Server
Local IP	Start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

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

- NAT Server Sets

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

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



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

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

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

Menu 15.2 - NAT Server Setup (Used for SUA Only)			
Rule	Start Port No.	End Port No.	IP Address
-----	-----	-----	-----
1.	Default	Default	0.0.0.0

2.	21	21	192.168.1.33
3.	80	80	192.168.1.36
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

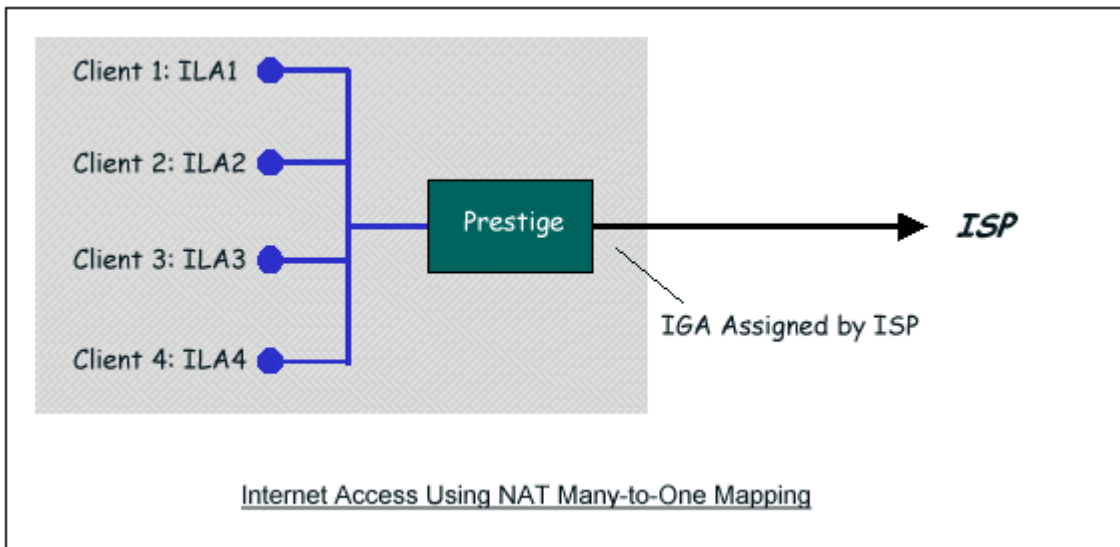
The most often used port numbers are shown in the following table. Please refer RFC 1700 for further information about port numbers.

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

---

### 1. Internet Access Only

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



Menu 4 - Internet Access Setup

```

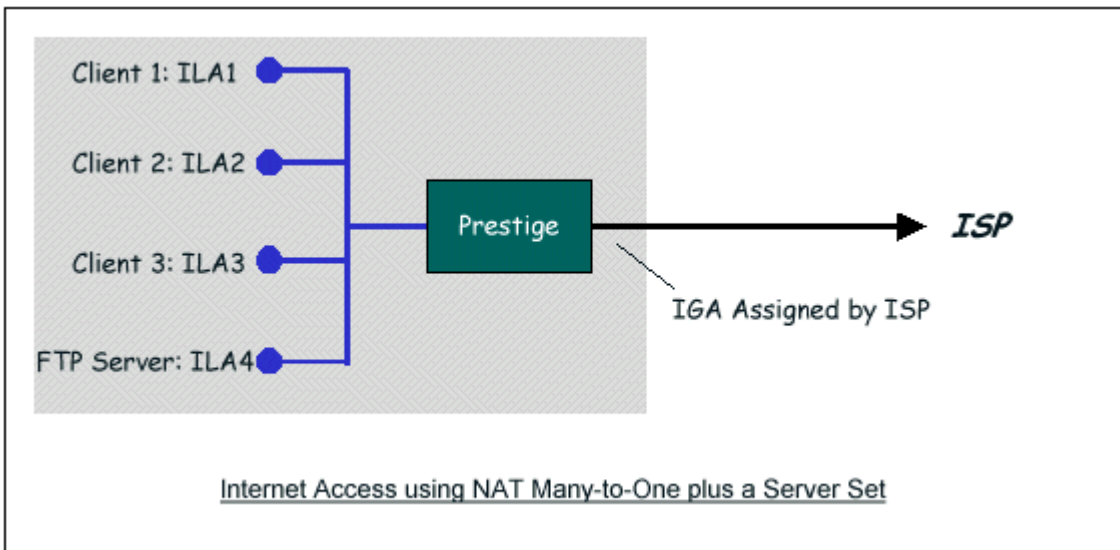
ISP's Name= MyISP
Encapsulation= PPPoE
Multiplexing= LLC-based
VPI #= 0
VCI #= 33
ATM QoS Type= UBR
    Peak Cell Rate (PCR)= 0
    Sustain Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
My Login= cso@zyxel
My Password= *****
Idle Timeout (sec)= 0
IP Address Assignment= Dynamic
    IP Address= N/A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

Press ENTER to Confirm or ESC to Cancel:



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

**2. Internet Access with an Internal Server**



In this case, we do exactly as above (use the convenient pre-configured SUA Only set) and also go to Menu 15.2-NAT Server Setup (Used for SUA Only) to specify the Internet Server behind the NAT as shown in the NAT as shown below.

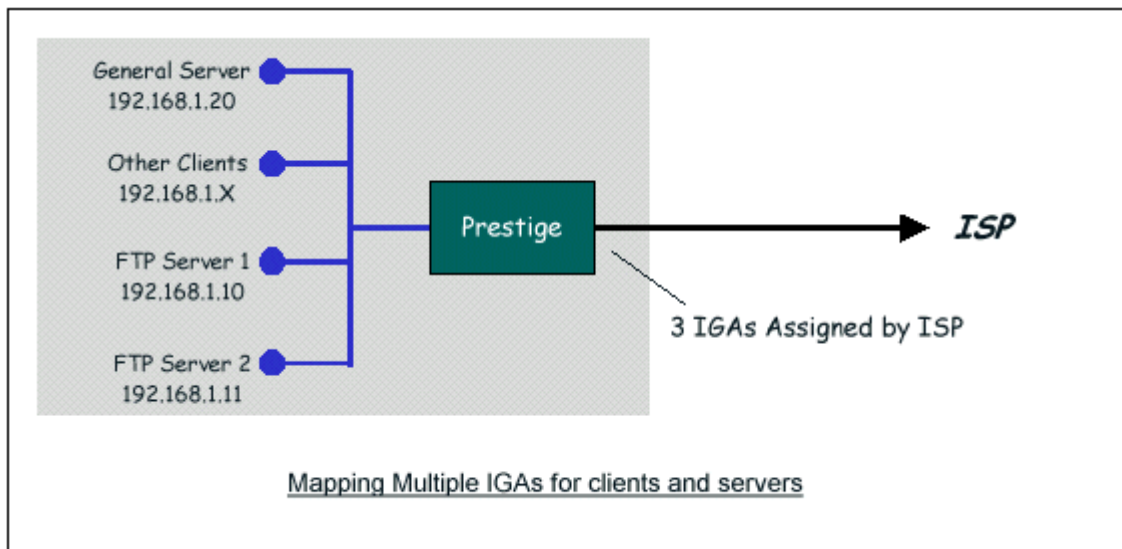
Menu 15.2 - NAT Server Setup (Used for SUA Only)

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

8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

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



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

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

Step 1:

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

Menu 4 - Internet Access Setup

```
ISP's Name= MyISP
Encapsulation= PPPoE
Service Type= N/A
My Login= cso@zyxel
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Static
IP Address= IGA3
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= Full Feature

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

Step 2:

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

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

```
Menu 15.1.1.1 - - Rule 1
Type: One-to-One
Local IP:
```

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

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

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

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

```
Menu 15.1.1.3 - - Rule 3
Type: Many-to-One
Local IP:
Start= 0.0.0.0
End  = 255.255.255.255
Global IP:
Start= [Enter IGA3]
End  = N/A
```

Press ENTER to Confirm or ESC to Cancel:

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

Menu 15.1.1.4 - - Rule 4

Type: **Server**

Local IP:

Start= N/A

End = N/A

Global IP:

Start= **[Enter IGA3]**

End = N/A

Press ENTER to Confirm or ESC to Cancel:

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

Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

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

- 9.
- 10.

Press ESC or RETURN to Exit:

Step 3:

Now we configure all other incoming traffic to go to our web server and mail server from **Menu 15.2 - NAT Server Setup** (not Set 1, Set 1 is used for SUA Only case).

Menu 15.2 - NAT Server Setup

Rule Start Port No. End Port No. IP Address

-----

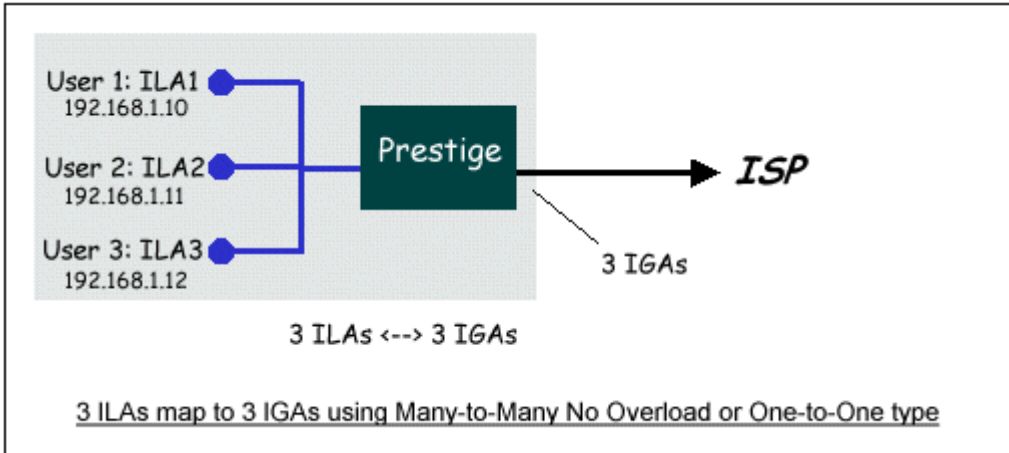
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.20
3.	25	25	192.168.1.20
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

---

#### 4. Support Non NAT Friendly Applications

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



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

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

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

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

```
Menu 15.1.1.1 - - Rule 1

Type: One-to-One
```

Local IP:  
Start= 192.168.1.10  
End = N/A

Global IP:  
Start= [Enter IGA1]  
End = N/A

Press ENTER to Confirm or ESC to Cancel:

Menu 15.1.1.2 - - Rule 2

Type: One-to-One

Local IP:  
Start= 192.168.1.11  
End = N/A

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

Press ENTER to Confirm or ESC to Cancel:

Menu 15.1.1.3 - - Rule 3

Type: One-to-One

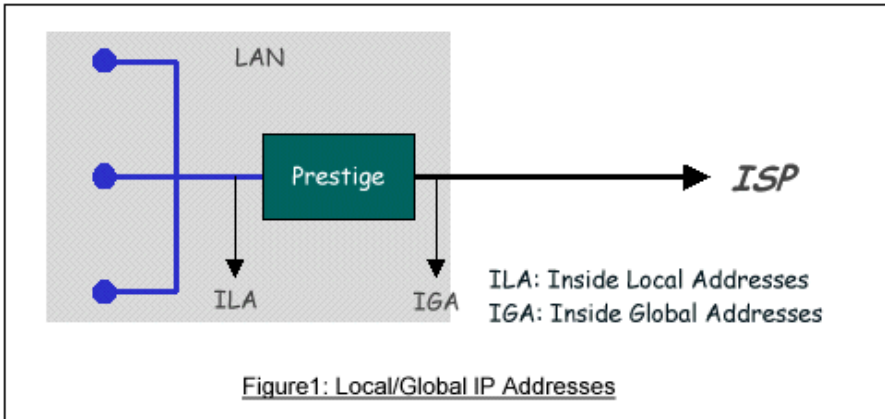
Local IP:  
Start= 192.168.1.12  
End = N/A

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



Press ENTER to Confirm or ESC to Cancel:

Prestige supports multiple type of NAT mapping rules



- 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

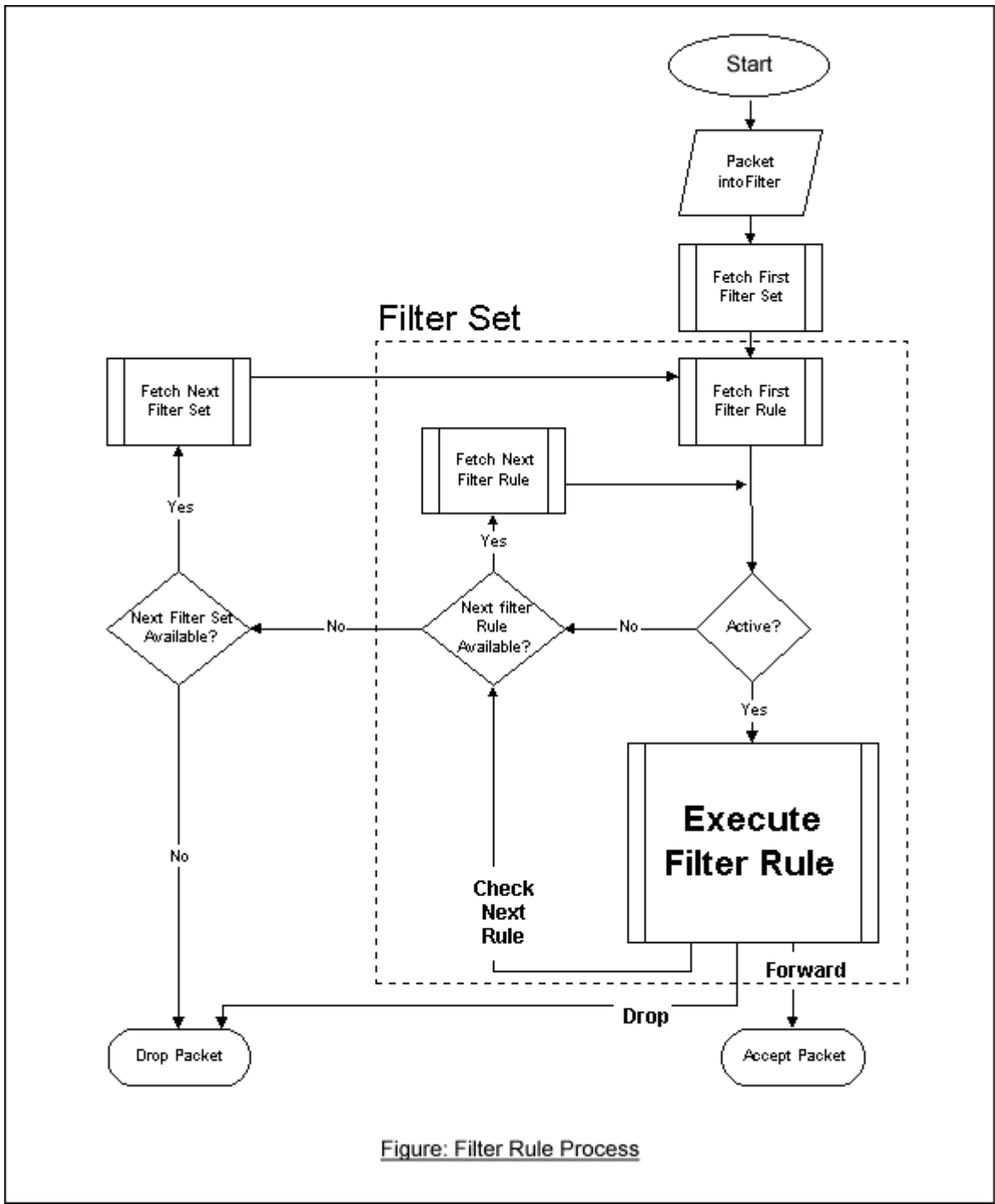
	...
Server (SUA)	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

## About Filter & Filter Examples

How does ZyXEL filter work?

- **Filter Structure**

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



- Filter Types and SUA**

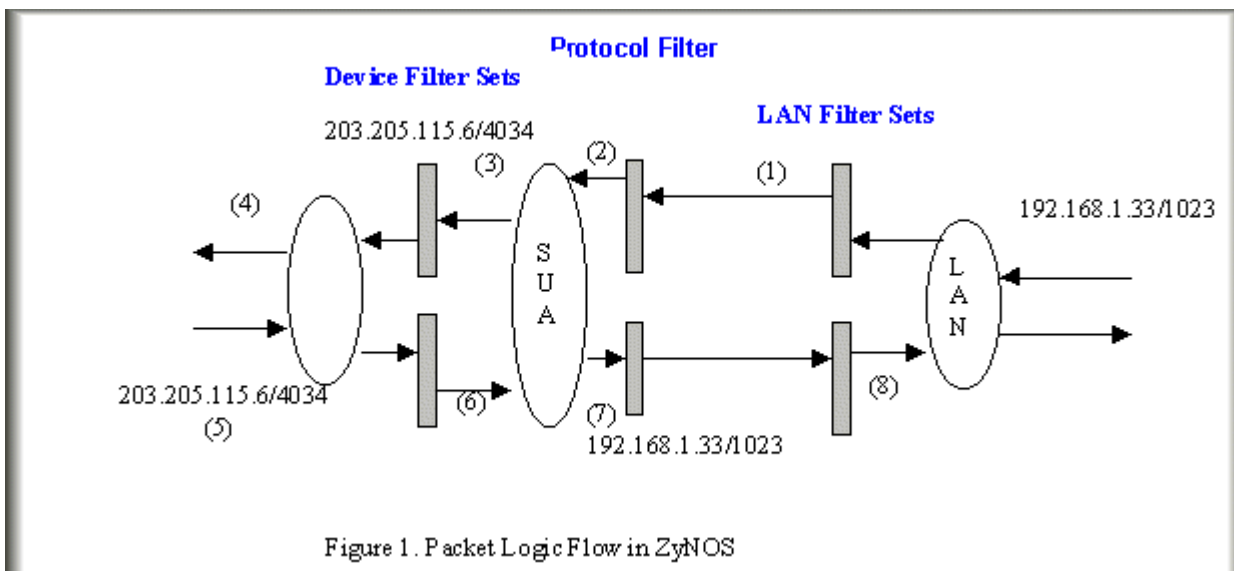
Conceptually, there are two categories of filter rules: **device** and **protocol**. The Generic filter rules belong to the device category; they act on the raw data from/to LAN and WAN. The IP and IPX filter rules belong to the protocol category; they act on the IP and IPX packets.

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

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

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

- WAN device input filter sets.
- If SUA is enabled, SUA converts the destination IP address from 203.205.115.6 to 92.168.1.33 and port number from 4034 to 1023.
- WAN protocol input filter sets.
- LAN device and protocol output filter sets.



**Generic** and **TCP/IP (and IPX)** filter rules are in different filter sets. The SMT will detect and prevent the mixing of different category rules within any filter set in Menu 21. In the following example, you will receive an error message '**Protocol and device filter rules cannot be active together**' if you try to activate a TCP/IP (or IPX) filter rule in a filter set that has already had one or more active Generic filter rules. You will receive the

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

Menu 21.1.1:

```
Menu 21.1.1 - Generic Filter Rule
Filter #: 1,1
Filter Type= Generic Filter Rule
Active= Yes
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No          Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule
```

Menu 21.1.2:

```
Menu 21.1.2 - TCP/IP Filter Rule
Filter #: 1,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0   IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
TCP Estab= N/A
```

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

Press ENTER to Confirm or ESC to Cancel:

Saving to ROM. Please wait...

**Protocol and device rule cannot be active together**

To separate the device and protocol filter categories; two new menus, Menu 11.5 and Menu 13.1, have been added, as well as some changes made to the Menu 3.1, Menu 11.1, and Menu 13. The new fields are shown below.

Menu 3.1:

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

Menu 11.1:

```
Menu 11.1 - Remote Node Profile

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

Encapsulation= PPP         Edit PPP Options= No
Incoming:                  Rem IP Addr= ?
Rem Login= test            Edit IP/IPX/Bridge= No
Rem Password= *****
```

```
Outgoing:                               Session Options:
My Login= testt                          Edit Filter Sets= Yes
My Password= *****
Authen= CHAP/PAP
      Press ENTER to Confirm or ESC to Cancel:
```

## Menu 11.5:

```
      Menu 11.5 - Remote Node Filter
Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
```

SMT will also prevent you from entering a protocol filter set configured in Menu 21 to the [device filters](#) field in Menu 3.1, 11.5, or entering a device filter set to the [protocol filters](#) field. Even though SMT will prevent the inconsistency from being entered in ZyNOS, it is unable to resolve the intermixing problems existing in the filter sets that were configured before. Instead, when ZyNOS translates the old configuration into the new format, it will verify the filter rules and log the inconsistencies. Please check the system log (Menu 24.3.1) before putting your device into use.

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

---

### filter for blocking the web service

- Configuration

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

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

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

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

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

- o Create a filter set in Menu 21, e.g., set 1
- o Create three filter rules in Menu 21.1.1, Menu 21.1.2, Menu 21.1.3
  - Rule 1- block the HTTP packet, TCP (06) protocol with port number 80
  - Rule 2- block the DNS packet, TCP (06) protocol with port number 53
  - Rule 3- block the DNS packet, UDP (17) protocol with port number 53
- o Apply the filter set in menu 4

1. Create a filter set in Menu 21

Menu 21 - Filter Set Configuration

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

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



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

```
Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 80
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        Port #=
        Port # Comp= None
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

```
Menu 21.1.2 - TCP/IP Filter Rule
Filter #: 1,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 53
                Port # Comp= Equal
```

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

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

```
Menu 21.1.2 - TCP/IP Filter Rule
Filter #: 1,2
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 completed, you will see the rule summary in Menu 21.

Menu 21.1 - Filter Rules Summary

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

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

### A filter for blocking a specific client

#### Configuration

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

Menu 21 - Filter Set Configuration

Filter Set #	Comments	Filter Set #	Comments
1	Block a client	7	_____
2	_____	8	_____
3	_____	9	_____
4	_____	10	_____
5	_____	11	_____
6	_____	12	_____

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

2. One rule for blocking all packets from this client

```
Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #-
                Port # Comp= None
Source: IP Addr= 192.168.1.5
        IP Mask= 255.255.255.255
        Port #-
        Port # Comp= None
TCP Estab= N/A
More= No           Log= None
Action Matched= Drop
Action Not Matched= Forward
Press ENTER to Confirm or ESC to Cancel:
```

### Key Settings:

Source IP addr.....Enter the client IP in this field

IP Mask.....here the IP mask is used to mask the bits of the IP address given in the **'Source IP Addr='** field, for one workstation it is 255.255.255.255.

Action Matched.....Set to 'Drop' to drop all the packets from this client

Action Not Matched.....Set to 'Forward' to allow the packets from other clients

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

---

## A filter for blocking a specific MAC address

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

### Before you Begin

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

```
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on
Now a client on the LAN is trying to ping Prestige.....
ras> sys trcp sw off
ras> sys trcp disp
TIME: 37c060 enet0-RECV len:74 call=0
0000: [00 a0 c5 01 23 45] [00 80 c8 4c ea 63] 08 00 45 00
0010: 00 3c eb 0c 00 00 20 01 e3 ea ca 84 9b 5d ca 84
0020: 9b 63 08 00 45 5c 03 00 05 00 61 62 63 64 65 66
0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040: 77 61 62 63 64 65 66 67 68 69
TIME: 37c060 enet0-XMIT len:74 call=0
0000: [00 80 c8 4c ea 63] [00 a0 c5 01 23 45] 08 00 45 00
0010: 00 3c 00 07 00 00 fe 01 f0 ef ca 84 9b 63 ca 84
0020: 9b 5d 00 00 4d 5c 03 00 05 00 61 62 63 64 65 66
0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040: 77 61 62 63 64 65 66 67 68 69
```

The detailed format of the Ethernet Version II:

```
+ Ethernet Version II
- Address: 00-80-C8-4C-EA-63 (Source MAC) ----> 00-A0-C5-23-45
  (Destination MAC)
- Ethernet II Protocol Type: IP
```

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

## Configurations

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

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

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

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

```
Menu 21.1.1 - Generic Filter Rule
Filter #: 1,1
Filter Type= Generic Filter Rule
Active= Yes
Offset= 6
Length= 6
Mask= ffffffff
Value= 0080c84cea63
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward
```

#### Key Settings:

- Generic Filter Ruls  
Set the 'Filter Type' to 'Generic Filter Rule'
- Active  
Turn 'Active' to 'Yes'
- Offset (in bytes)  
Set to '6' since the source MAC address starts at 7th octets we need to skip the first octets of the destination MAC address.
- Length (in bytes)  
Set to '6' since MAC address has 6 octets.
- Mask (in hexadecimal)  
Specify the value that the Prestige will logically qualify (logical AND) the data in the packet. Since the Length is set to 6 octets the Mask for it should be 12 hexadecimal numbers. In this case, we intent to set to 'ffffffff' 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 matched.

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

```
Menu 21.1.2 - Generic Filter Rule
Filter #: 1,2
Filter Type= Generic Filter Rule
Active= Yes
Offset= 6
Length= 6
Mask= ffffffff
Value= 0080c810234a
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward
```

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

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



## A filter for blocking the NetBIOS packets

- Introduction

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

- Configuration

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

Filter Set 1:

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

Filter Set 2:

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

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

Menu 21 - Filter Set Configuration

Filter

Filter

Set #	Comments	Set #	Comments
1	NetBIOS_WAN	7	_____
2	NetBIOS_LAN	8	_____
3	_____	9	_____
4	_____	10	_____
5	_____	11	_____
6	_____	12	_____

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

Configure the first filter set 'NetBIOS\_WAN' by selecting the Filter Set number 1.

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

Menu 21.1.1 - TCP/IP Filter Rule  
Filter #: 1,1  
Filter Type= TCP/IP Filter Rule  
Active= Yes  
IP Protocol= 6      IP Source Route= No  
Destination: IP Addr= 0.0.0.0  
                  IP Mask= 0.0.0.0  
                  Port #= 137  
                  Port # Comp= Equal  
Source: IP Addr= 0.0.0.0  
                  IP Mask= 0.0.0.0  
                  Port #= 0  
                  Port # Comp= None  
TCP Estab= No  
More= No            Log= None  
Action Matched= Drop  
                  Action Not Matched= Check Next Rule  
Press ENTER to Confirm or ESC to Cancel:

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

```
Menu 21.1.2 - TCP/IP Filter Rule
Filter #: 1,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17    IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 137
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
         IP Mask= 0.0.0.0
         Port #= 0
         Port # Comp= None
TCP Estab= N/A
More= No          Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

```
Menu 21.1.3 - TCP/IP Filter Rule
Filter #: 1,3
Filter Type= TCP/IP Filter Rule
Active= Yes
```

```
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                  IP Mask= 0.0.0.0
                  Port #= 138
                  Port # Comp= Equal
Source: IP Addr= 0.0.0.0
          IP Mask= 0.0.0.0
          Port #= 0
          Port # Comp= None

TCP Estab= No
More= No      Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule

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

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

```
Menu 21.1.4 - TCP/IP Filter Rule
Filter #: 1,4
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17    IP Source Route= No
Destination: IP Addr= 0.0.0.0
                  IP Mask= 0.0.0.0
                  Port #= 138
                  Port # Comp= Equal
Source: IP Addr= 0.0.0.0
          IP Mask= 0.0.0.0
          Port #= 0
          Port # Comp= None

TCP Estab= N/A
More= No      Log= None
```

```
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

```
Menu 21.1.5 - TCP/IP Filter Rule
Filter #: 1,5
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 139
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
         IP Mask= 0.0.0.0
         Port #= 0
         Port # Comp= None
TCP Estab= No
More= No      Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

```
Menu 21.1.6 - TCP/IP Filter Rule
Filter #: 1,6
```

```
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17    IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 139
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
          IP Mask= 0.0.0.0
          Port #= 0
          Port # Comp= None

TCP Estab= N/A
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward

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

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

Menu 21.2 - Filter Rules Summary			
#	A Type	Filter Rules	M m n
1	Y IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137	N D N
2	Y IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137	N D N
3	Y IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138	N D N
4	Y IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138	N D N
5	Y IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139	N D N
6	Y IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139	N D F

- Apply the first filter set 'NetBIOS\_WAN' to the **'Output Protocol Filter'** in the remote node setup.

Configure the second filter set 'NetBIOS\_LAN' by selecting the Filter Set number 2.

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

```
Menu 21.2.1 - TCP/IP Filter Rule
Filter #: 2,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 53
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        Port #= 137
        Port # Comp= Equal
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

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

```

Menu 21.2 - Filter Rules Summary
# A Type          Filter Rules          M m n
-----
1 Y IP   Pr=6, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53  N D N
2 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53  N D F
    
```

1. Apply the filter set 'NetBIOS\_LAN' in the **'Input protocol filters='** in the Menu 3 for blocking the packets from LAN

Menu 3.1 - General Ethernet Setup

Input Filter Sets:



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

## Using the Dynamic DNS (DDNS)

### 1. What is DDNS?

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

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

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

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

The DDNS servers the Prestige supports currently is [WWW.DYNDNS.ORG](http://WWW.DYNDNS.ORG) where you apply the DNS from and update the WAN IP to.

- Setup the DDNS
- Before configuring the DDNS settings in the Prestige, you must register an account from the DDNS server such as [WWW.DYNDNS.ORG](http://WWW.DYNDNS.ORG) first. After the registration, you have a hostname for your internal server and a password using to update the IP to the DDNS server.
- Toggle '**Configure Dynamic DNS**' option to '**Yes**' and press ENTER for configuring the settings of the DDNS in menu 1.1.

Menu 1 - General Setup

System Name= Prestige  
 Location=  
 Contact Person's Name=  
 Domain Name=  
 Edit Dynamic DNS= **Yes**

Route IP= Yes  
 Bridge= No

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG  
 Active= **Yes**  
 Host=[**the local server's host name**]  
 EMAIL=  
 USER=  
 Password= \*\*\*\*\*  
 Enable Wildcard= No

Key Settings for using DDNS function:

Option	Description
<b>Service Provider</b>	Enter the DDNS server in this field. Currently, we support <a href="http://WWW.DYNDNS.ORG">WWW.DYNDNS.ORG</a> .
<b>Active</b>	Toggle to 'Yes'.
<b>Host</b>	Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw.
<b>EMAIL</b>	Enter the email address you give to the DDNS server.
<b>User</b>	Enter the user name that

<b>Password</b>	Enter the password that the DDNS server gives to you.
<b>Enable Wildcard</b>	Enter the hostname for the wildcard function that the <a href="http://WWW.DYNDNS.ORG">WWW.DYNDNS.ORG</a> supports. Note that Wildcard option is available only when the provider is <a href="http://WWW.DYNDNS.ORG">WWW.DYNDNS.ORG</a> .

## Network Management Using SNMP

### 1. *SNMP Overview*

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

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

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

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

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

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

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

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

#### 6. Reads

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

#### 7. Writes

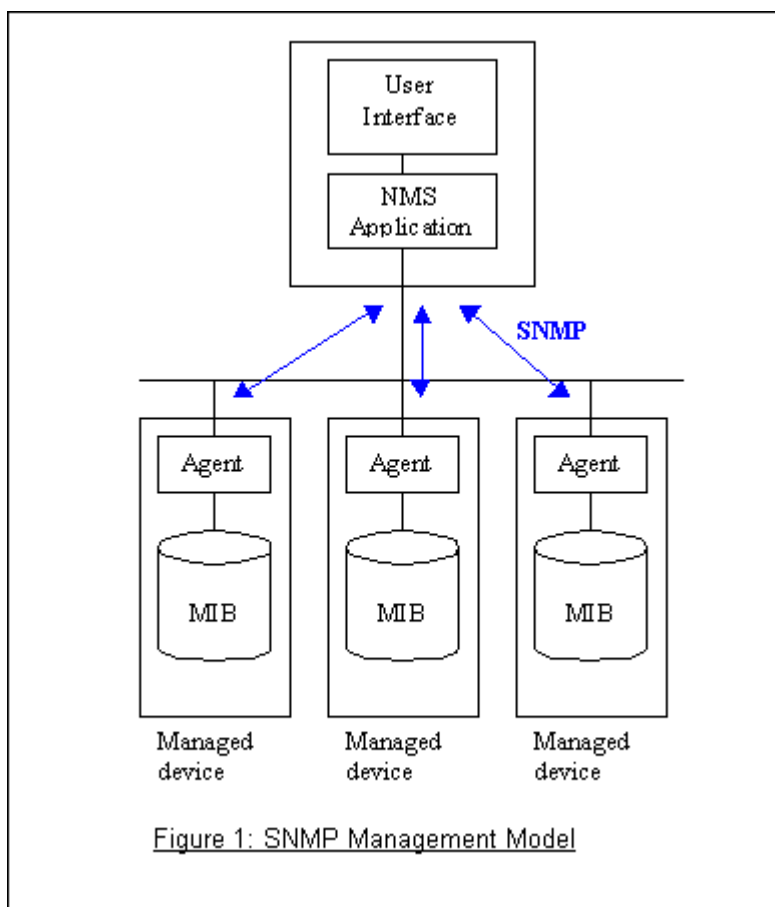
Write is used to control the managed devices, NMSs write variables that are stored in the managed devices.

#### 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 to asynchronously report certain events to NMSs use trap.



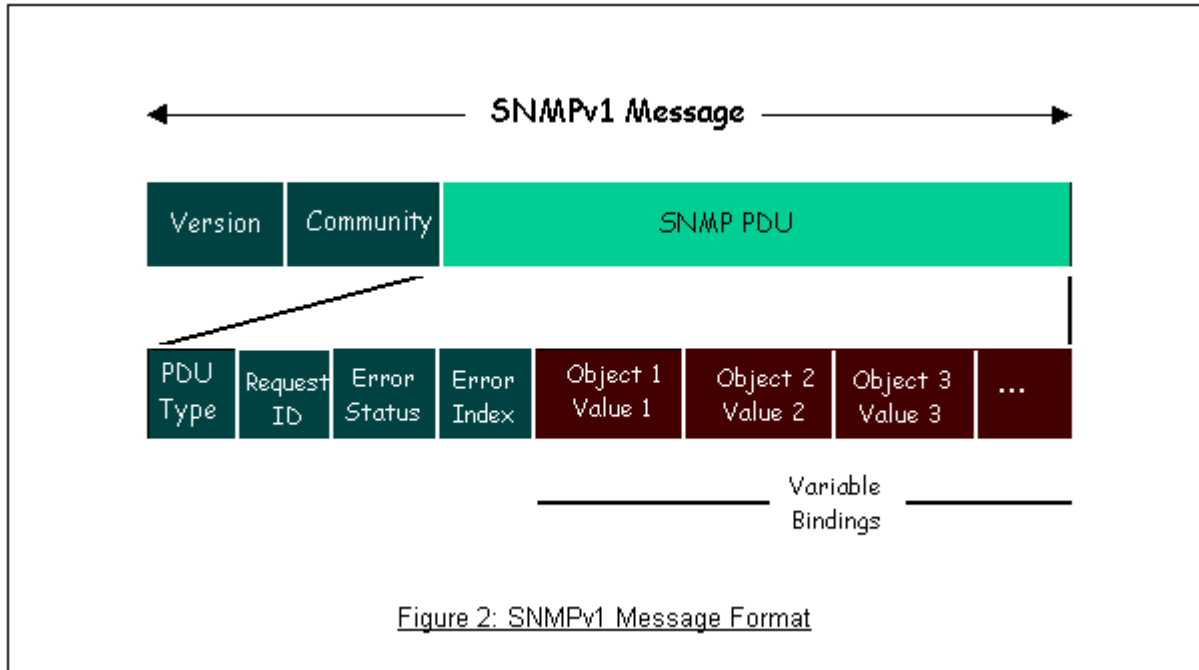
## 2. SNMPv1 Operations

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

- **Get**  
Allows the NMS to retrieve an object variable from the agent.
- **GetNext**  
Allows the NMS to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a NMS wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- **Set**  
Allows the NMS to set values for object variables within an agent.
- **Trap**  
Used by the agent to inform the NMS of some events.

The SNMPv1 messages contains two part. The first part contains a version and a community name. The second part contains the actual SNMP protocol data unit (PDU) specifying the operation to be performed (Get, Set, and

so on) and the object values involved in the operation. The following figure shows the SNMPv1 message format.



The SNMP PDU contains the following fields:

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

### 3. ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some Prestige routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. For SNMPv1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

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

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

- **linkUp** (defined in RFC-1215) :

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

- **authenticationFailure** (defined in RFC-1215) :

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

1. **whyReboot** (defined in ZYXEL-MIB) :

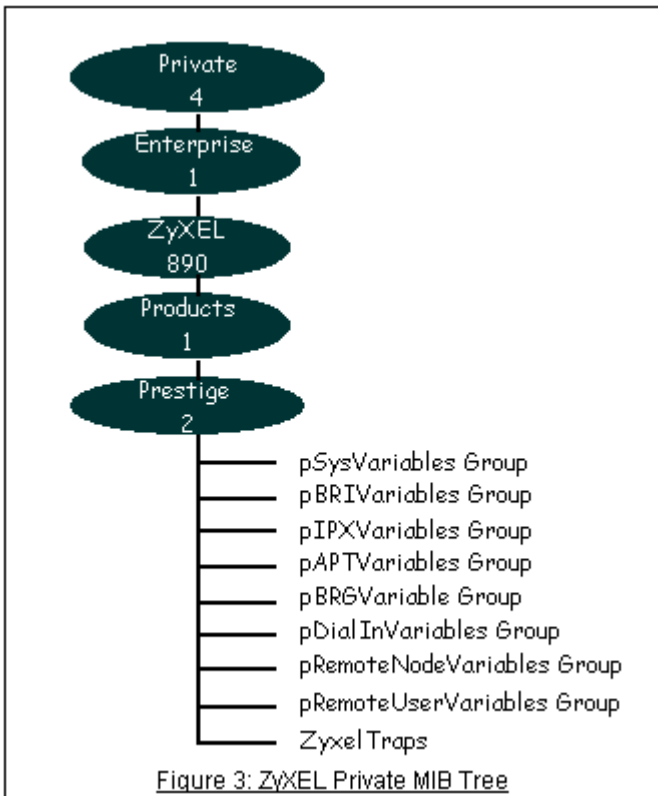
When the system is going to restart (warmstart), the trap will be sent with the reason of restart before rebooting.

(i) For intentional reboot :

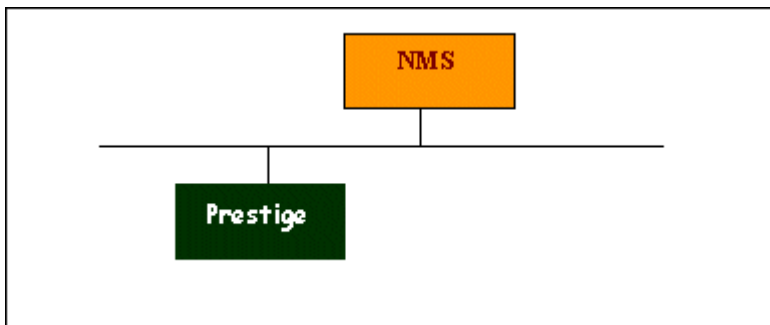
In some cases (download new files, CI command "sys reboot", ...), reboot is done intentionally. And traps with the message "System reboot by user !" will be sent.

(ii) For fatal error :

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



*4. Configure the Prestige for SNMP*



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

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



```
Trap:  
Community= public  
Destination= 192.168.1.33  
  
Press ENTER to Confirm or ESC to Cancel:
```

Key Settings:

Option	Descriptions
<b>Get Community</b>	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
<b>Set Community</b>	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
<b>Trusted Host</b>	Enter the IP address of the NMS. The Prestige will only respond to SNMP messages coming from this IP address. <b>If 0.0.0.0 is entered, the Prestige will respond to all NMS managers.</b>
<b>Trap Community</b>	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'.
<b>Trap Destination</b>	Enter the IP address of the NMS that you wish to send the traps to. <b>If 0.0.0.0 is entered, the Prestige will not send trap any NMS manager.</b>

## 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**, use the space bar to turn on the syslog option.
2. **Syslog IP Address**, enter the IP address of the UNIX server that you wish to send the syslog.
3. **Log Facility**, use the space bar to toggle between the 7 different local options.

- **UNIX Setup**

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

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

2. Edit the file [/etc/syslog.conf](#) by adding the following line at the end of the [/etc/syslog.conf](#) file.

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

Where [/var/log/zyxel.log](#) is the full path of the log file.

3. Restart syslogd.

- **CDR log(call messages)**

Format:

```
sdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );
```

String = board xx line xx channel xx, call xx, str

board = the hardware board ID

line = the WAN ID in a board

channel = channel ID within the WAN

call = the call reference number which starts from 1 and increments by 1 for each new call

str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)

C01 Incoming Call xxxxBps xxxxx (L2TP,xxxxx means Remote Call ID)

C01 Incoming Call xxxx (means connected speed) xxxxx (means Remote Call ID)

L02 Tunnel Connected(L2TP)

C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call ID)

C02 CLID call refused

L02 Call Terminated

C02 Call Terminated

Example:

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

- **Packet triggered log**

Format:

```
sdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
```

String = Packet trigger: Protocol=xx Data=xxxxxxxxxx

Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)

Data: We will send forty-eight Hex characters to the server

Example:

```
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd40000020405b4
```

- **Filter log**

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

Format:

```
sdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
```

String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx]S04>R01mD

IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).

Src: Source Address

Dst: Destination Address

prot: Protocol (TCP,UDP,ICMP)

spo: Source port

dpo: Destination port

Example:

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

- **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

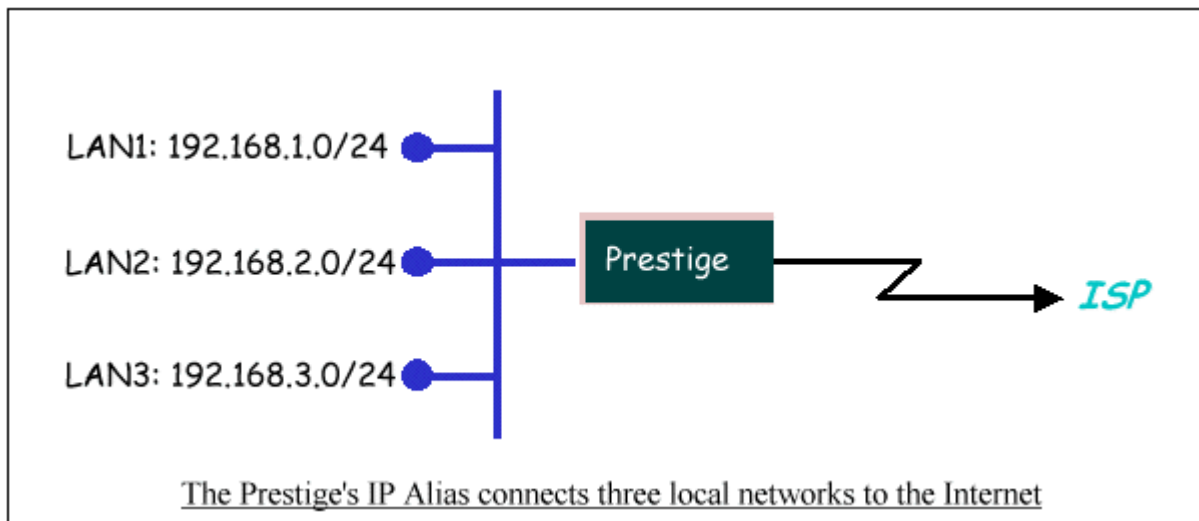
Example:

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



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

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

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

- **IP Alias Setup**

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

Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup

DHCP= Server

Client IP Pool Starting Address= **192.168.1.33**

Size of Client IP Pool= 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:

Key Settings:

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

<b>Edit IP Alias</b>	Toggle to 'Yes' to enter menu 3.2.1 for setting up the second and third networks.
----------------------	---

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

```
Menu 3.2.1 - IP Alias Setup
IP Alias 1= Yes
  IP Address= 192.168.2.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
  Version= RIP-1
  Incoming protocol filters=
  Outgoing protocol filters=
IP Alias 2= Yes
  IP Address= 192.168.3.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
  Version= RIP-1
  Incoming protocol filters=
  Outgoing protocol filters=

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

Key Settings:

<b>IP Alias 1</b>	Toggle to 'Yes' and enter the second LAN IP address for the Prestige. This will create the second route in the enif0:0 interface.
<b>IP Alias 2</b>	Toggle to 'Yes' and enter the third LAN IP address for the Prestige. This will create the third route in the enif0:1 interface.

### Using Call Scheduling

1. What is Call Scheduling ?

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

- **SMT Menu for Call Scheduling**

1. Edit the Schedule sets in menu 26:

```
Prestige 2602HWL-61C 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 Password
  4. Internet Access Setup                     24. System Maintenance
                                              25. IP Routing Policy Setup
Advanced Applications                          26. Schedule Setup
  11. Remote Node Setup
  12. Static Routing Setup
  15. NAT Setup                               99. Exit

Enter Menu Selection Number:
```

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

```
Menu 26 - Schedule Setup

Schedule                                     Schedule
Set # Name                                  Set # Name
-----
 1 ZyXEL                                     7 _____
 2 _____                                8 _____
 3 _____                                9 _____
```



4 \_\_\_\_\_ 10 \_\_\_\_\_  
5 \_\_\_\_\_ 11 \_\_\_\_\_  
6 \_\_\_\_\_ 12 \_\_\_\_\_

Enter Schedule Set Number to Configure= 1

Edit Name= ZyXEL

Press ENTER to Confirm or ESC to Cancel:

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

#### Menu 26.1 Schedule Set Setup

Active= Yes

Start Date(yyyy-mm-dd)= 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:

### Key Settings:

<b>Start Date</b>	Start date of this schedule rule. It can be unmatched with weekday setting. For example, if Start Date is 2004/10/02(Monday), but Monday setting in weekday can be No.
<b>How Often</b>	If once is selected, all weekday settings will ne marked as N/A. After the rule is completely, it will be deleted automatically.
<b>Forced On</b>	The node will always keep up during the setting period. It is equivalent to diable the idel timeout.
<b>Forced Down</b>	The node will always keep doen during the setting period. The connected remote node will be dropped.
<b>Enable Dial-On-Demand</b>	The remote node accepts Dial-on-demand during this period.
<b>Disable Dial-On-Demand</b>	The remote node denies any demand dial during the period. For the existing connected nodes, it will be dropped after idle timeout and no triggered up.
<b>Start Time/Duration</b>	Start Time and Duration of this schedule.

- Apply the schedule to the Remote node

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

Menu 11.1 - Remote Node Profile

```

Rem Node Name= 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:

---

- **Time Service in Prestige**

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

Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= **Daytime (RFC-867)**

Time Server IP Address= **202.132.154.1**

Current Time: 00 : 11 : 38

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

Current Date: 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 to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the Prestige queries all directly connected networks to gather group membership.

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

- IP Multicast Setup

Enable IGMP in Prestige's LAN in menu 3.2:

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

#### DHCP Setup

DHCP= Server

Client IP Pool Starting Address= 192.168.1.33

Size of Client IP Pool= 32

Primary DNS Server= 0.0.0.0

Secondary DNS Server= 0.0.0.0

Remote DHCP Server= N/A

#### TCP/IP Setup:

IP Address= 192.168.1.1

```
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
  Version= RIP-2B
Multicast= IGMP-v2
IP Policies=
Edit IP Alias= No
```

Press ENTER to Confirm or ESC to Cancel:

Enable IGMP in Prestige's remote node in menu 11.3:

Menu 11.3 - Remote Node Network Layer Options

IP Options:

```
IP Address Assignment = Dynamic
Rem IP Addr = 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= N/A
NAT= SUA Only
  Address Mapping Set= N/A
Metric= 2
Private= No
RIP Direction= None
  Version= RIP-2B
Multicast= IGMP-v2
IP Policies=
```

Bridge Options:

```
Ethernet Addr Timeout(min)= N/A
```

Enter here to CONFIRM or ESC to CANCEL:

Key Settings:

<b>Multicast</b>	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2.
------------------	---

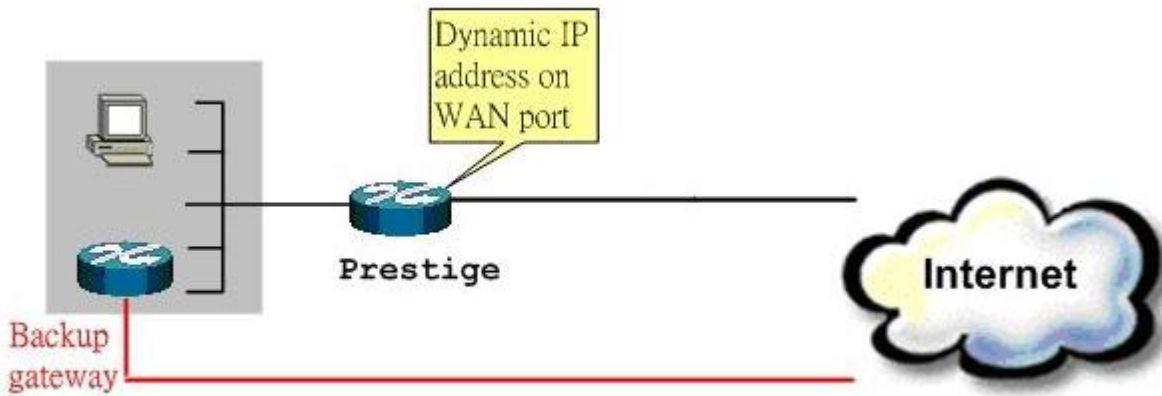
**Using Prestige traffic redirect**

- What is Traffic Redirect ?

Traffic redirect forwards WAN traffic to a backup gateway when Prestige cannot connect to the Internet through its normal gateway. Thus make your backup gateway as an auxiliary backup of your WAN connection. Once Prestige detects its WAN connectivity is broken, Prestige will try to forward outgoing traffic to backup gateway that users specify in traffic redirect configuration menu.

- How to deploy backup gateway?

You can deploy the backup gateway on LAN of Prestige.



**Traffic Redirect on LAN port**

---

- Traffic Redirect Setup

Configure parameters that determine when Prestige will forward WAN traffic to the backup gateway using SMT Menu 2 WAN Backup Setup.

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**

Key Settings:

Label	Description
<b>Backup Type</b>	Select the method that the Prestige uses to check the DSL connection.  Select <b>DSL Link</b> to have the Prestige check if the connection to the DSLAM is up. Select <b>ICMP</b> to have the Prestige periodically ping the IP addresses configured in the <b>Check WAN IP Address</b> fields.
<b>Check WAN IP Address1-3</b>	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).  <b>If you select ICMP in the Backup Type field, you must configure at least one IP address here.</b>  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.
<b>Fail Tolerance</b>	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the <b>Check WAN IP Address</b> fields without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
<b>Recovery Interval</b>	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to 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.
<b>Timeout</b>	Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the <b>Check WAN IP Address</b> fields before timing out the request. The WAN connection is considered "down" after the Prestige times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.
<b>Traffic</b>	

Label	Description
<b>Redirect</b>	
<b>Active</b>	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down.  <b>If you activate traffic redirect, you must configure at least one</b> Check WAN IP Address.
<b>Metric</b>	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".
<b>Backup Gateway</b>	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.
<b>Back</b>	Click <b>Back</b> to return to the previous screen.
<b>Apply</b>	Click <b>Apply</b> to save the changes.
<b>Cancel</b>	Click <b>Cancel</b> to begin configuring this screen afresh.

## Using Universal Plug n Play (UPnP)

- **1. What is UPnP**

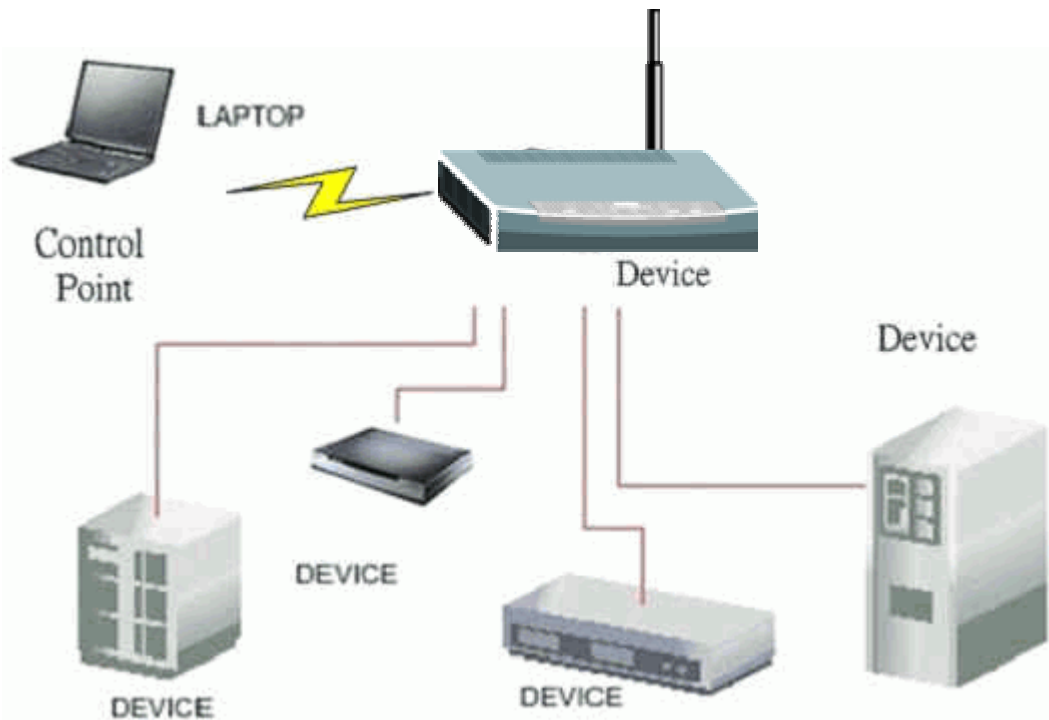
UPnP (Universal Plug and Play) makes connecting PCs of all form factors, intelligent appliances, and wireless devices in the home, office, and everywhere in between easier and even automatic by leveraging TCP/IP and Web technologies. UPnP can be supported on essentially any operating system and works with essentially any type of physical networking media – wired or wireless.

UPnP also supports NAT Traversal which can automatically solve many NAT unfriendly problems. By UPnP, applications assign the dynamic port mappings to Internet gateway and delete the mappings when the connections are complete.

The key components in UPnP are devices, services, and control points.



- **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.



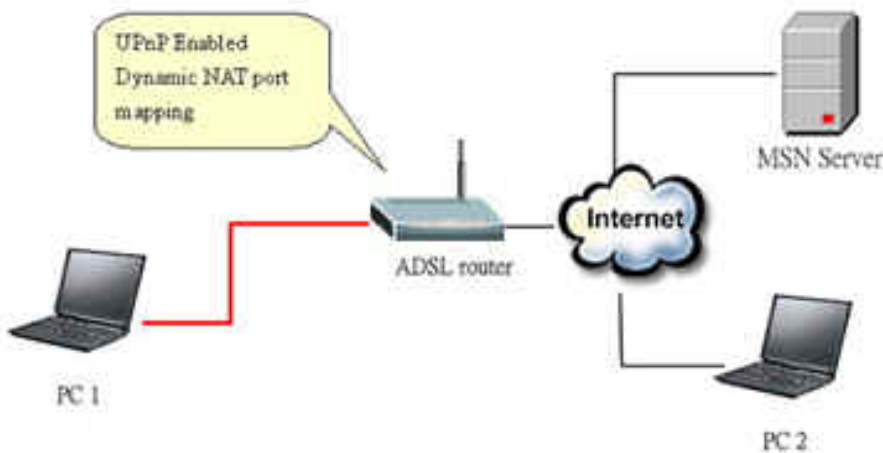
#### UPnP Operations

- **Addressing:** UPnPv1 devices MAY support IPv4, IPv6, or both. For IPv4, each device should have DHCP client, when the device gets connected to the network, it will discover DHCP server on network to get an IP address. If not, then Auto-IP mechanism should be supported so that the device can give itself an IP address.(169.254.0.0/16)
- **Discovery:** Whenever a device is added on the network, it will advertise its service over the network. Control point can also discover services provided by devices.
- **Description:** Control points can get more detailed service information from devices' description in XML format. The description may include product name, model name, serial number, vendor ID, and embedded services...etc.
- **Control:** Devices can be manipulated by control points through Control message.

- **Eventing:** Devices can send event message to notify control points if there is any update on services provided.
- **Presentation:** Each device can provide their own control interface by URL link. So that users can go to the device's presentation web page by the URL to control this device.
- **2. Using UPnP in ZyXEL devices**

In this example, we will introduce how to enable UPnP function in ZyXEL devices. Currently, Microsoft MSN is the most popular application exploiting UPnP, so we take Microsoft MSN application as an example in this support note. You can learn how MSN benefit from NAT traversal feature in UPnP in this application note.

In the diagram, suppose PC1 and PC2 both sign in MSN server, and they would like to establish a video conference. PC1 is behind PPPoE dial-up router which supports UPnP. Since the router supports UPnP, we don't need to setup NAT mapping for PC1. As long as we enable UPnP function on the router, PC1 will assign the mapping to the router dynamically. Note that since PC1 must support UPnP, we presume that it's OS is Microsoft WinME or WinXP.



Device: Prestige Router

Service: NAT function provided by Prestige Router

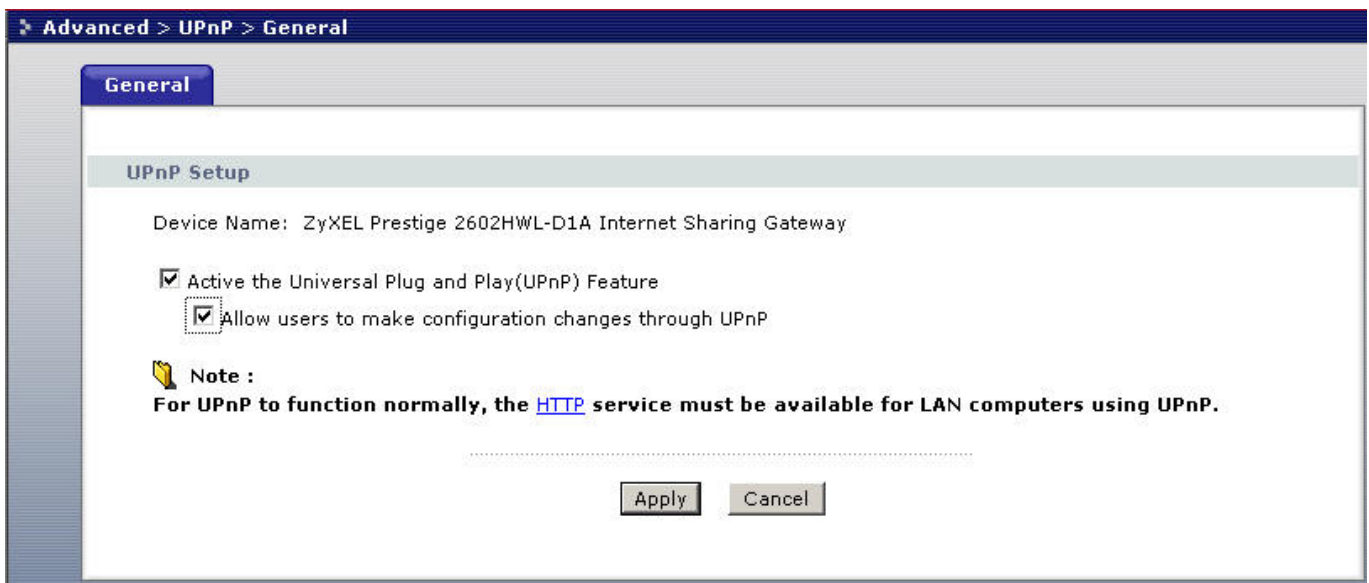
Control Point: PC1

1. Enable UPnP function in ZyXEL device

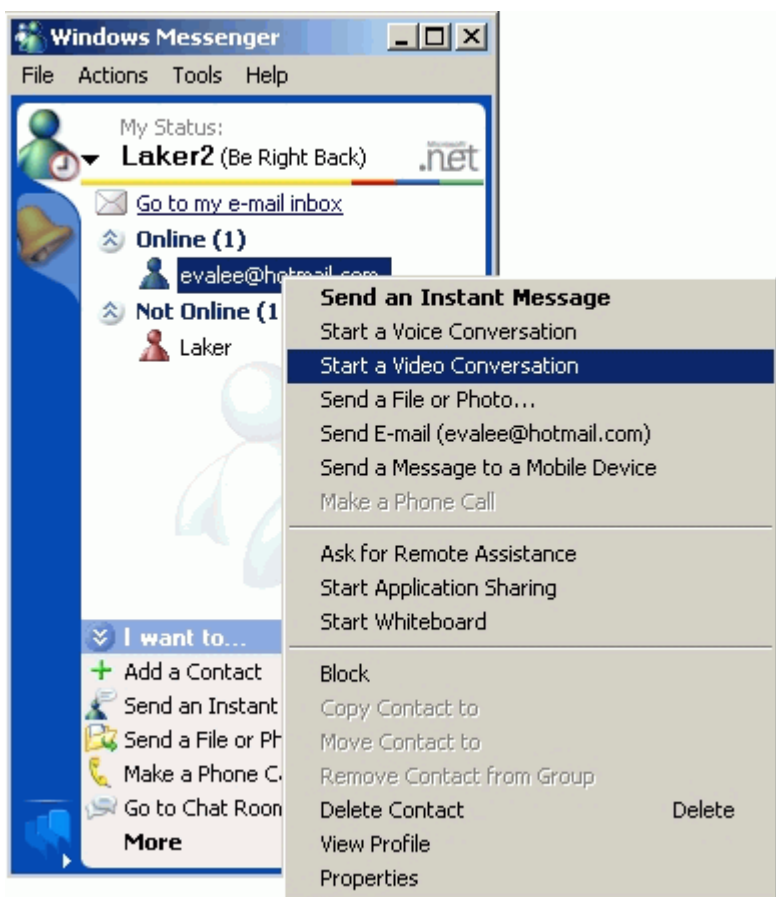
Go to **Advanced->UPnP**, check two boxes, **Active UPnP feature** and **Allow users to make configuration changes through UPnP**.

The first check box enables UPnP function in this device.

The second check box allow users' application to change configuration in this device. For instance, if you enable this item, then user's MSN application can assign dynamic port mapping to the router. So that network administrator don't need to setup SUA port mapping in the router.

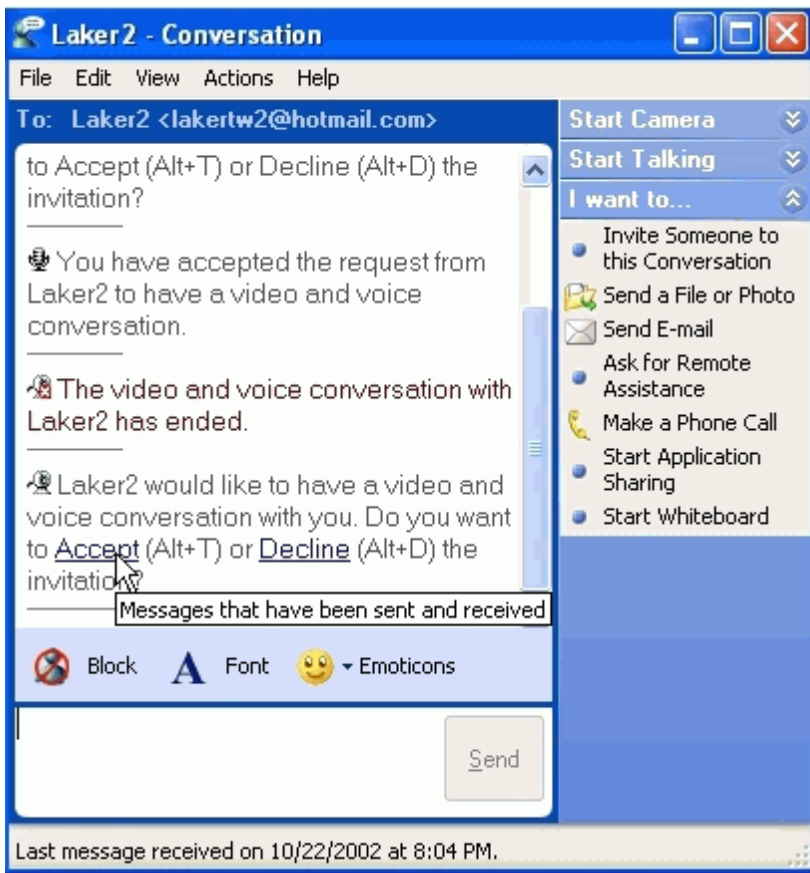


2. After getting IP address, you can go to open MSN application on PC and sign in MSN server.

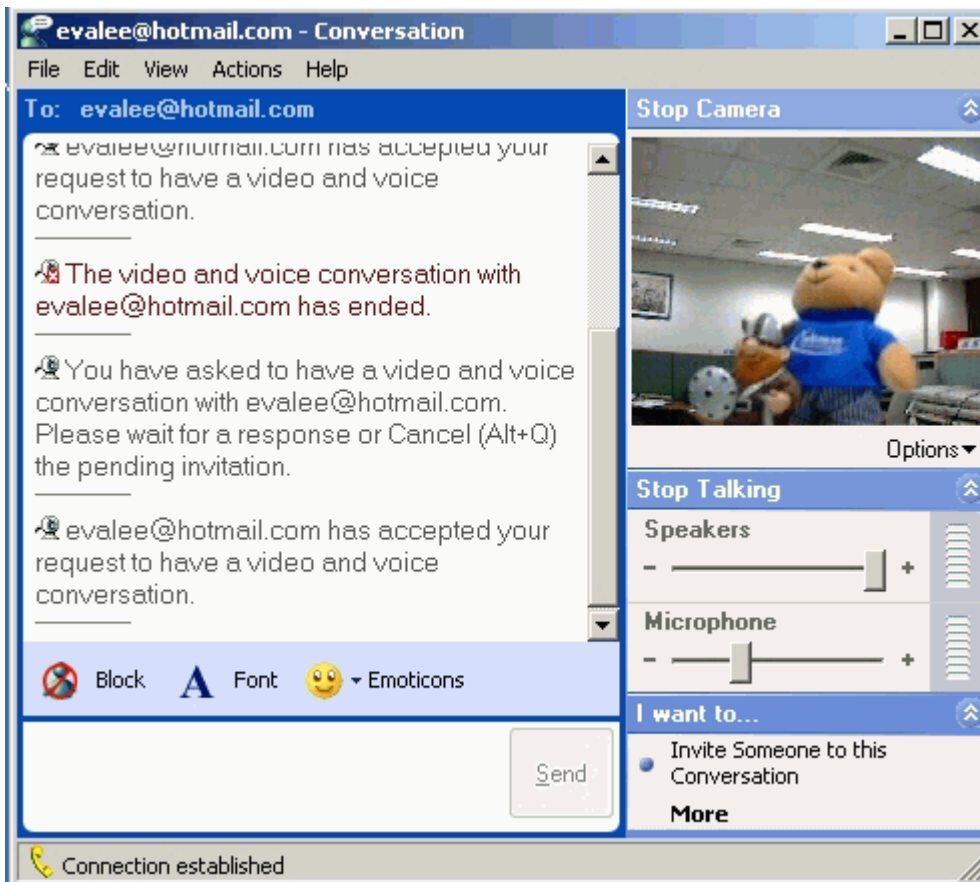


3. Start a Video conversation with one online user.

4. On the opposite side, your partner select **Accept** to accept your conversation request.



5. Finally, your video conversation is achieved.



## Wireless Application Notes (For Wireless Model Only)

### Infrastructure mode

What is Infrastructure mode?

Infrastructure mode, sometimes referred to as Access Point mode, is an operating mode of an 802.11b/Wi-Fi client unit. In infrastructure mode, the client unit can associate with an 802.11b/Wi-Fi Access Point and communicate with other clients in infrastructure mode through that access point.



---

### *Configuration Prestige Wireless using SMT.*

To configure Infrastructure mode of your Prestige wireless VoIP IAD please follow the steps below.

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= Wireless
Hide ESSID= No
Channel ID= CH07 2442MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= Disable
  Default Key= N/A
  Key1= N/A
  Key2= N/A
  Key3= N/A
  Key4= N/A
```

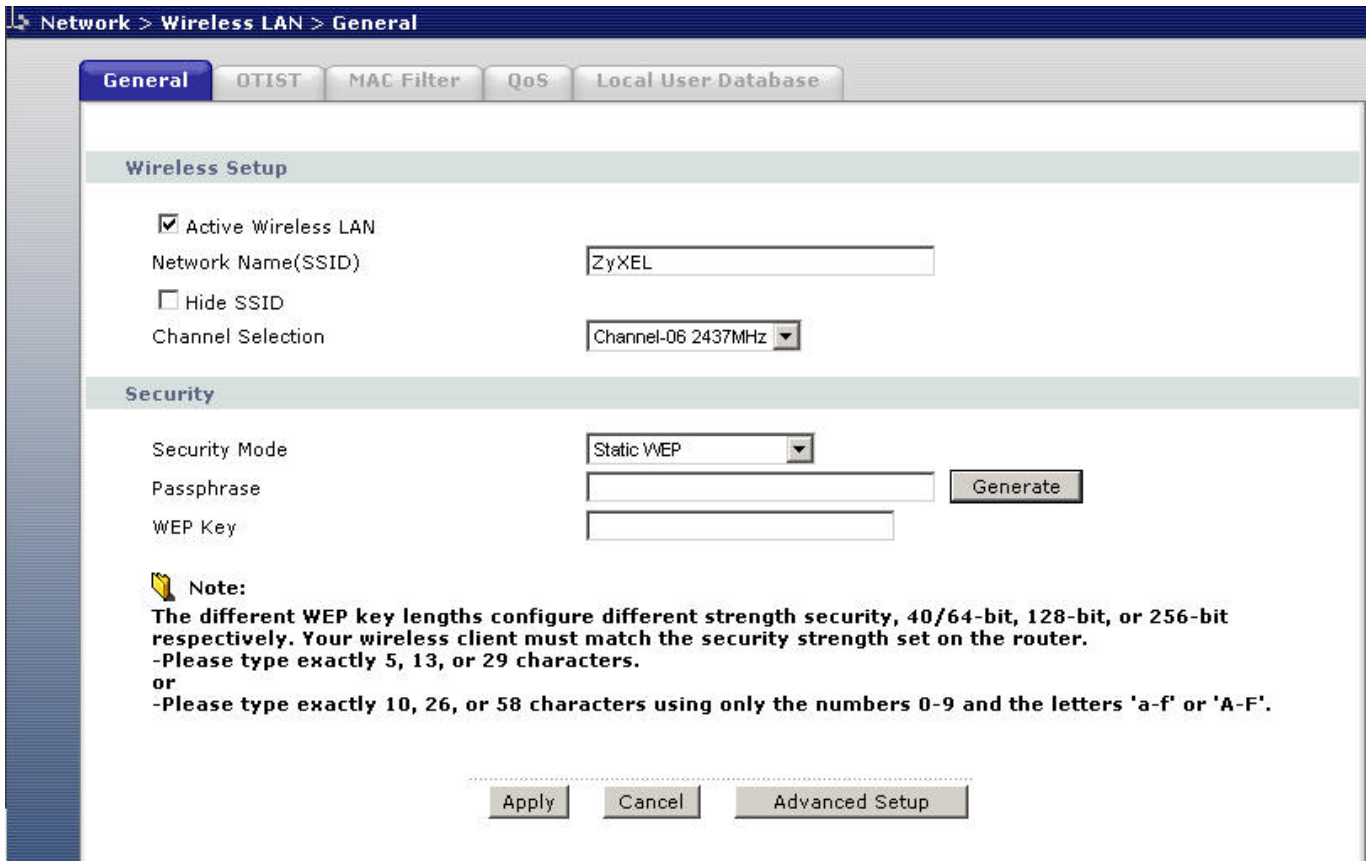
Edit MAC Address Filter= No  
Press ENTER to Confirm or ESC to Cancel:

3. Configure ESSID, Channel ID, WEP, Default Key and Keys as yo desire.

*Configuration Wireless Access Point to Infrastructure mode using Web configurator.*

To configure Infrastructure mode of your Prestige wireless VoIP IAD please follow the steps below.

1. From the web configurator main menu, click Network->>wireless LAN to display - Wireless LAN.



3. Configure the desired configuration on Prestige wireless VoIP IAD and check the **Active wireless LAN** check box.

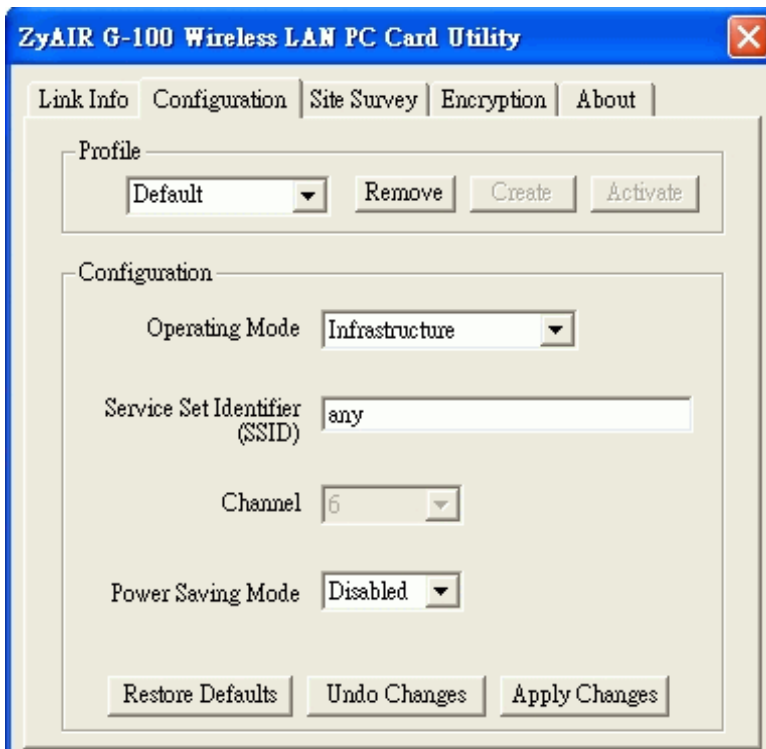
4. When finish click on apply button to take effect.



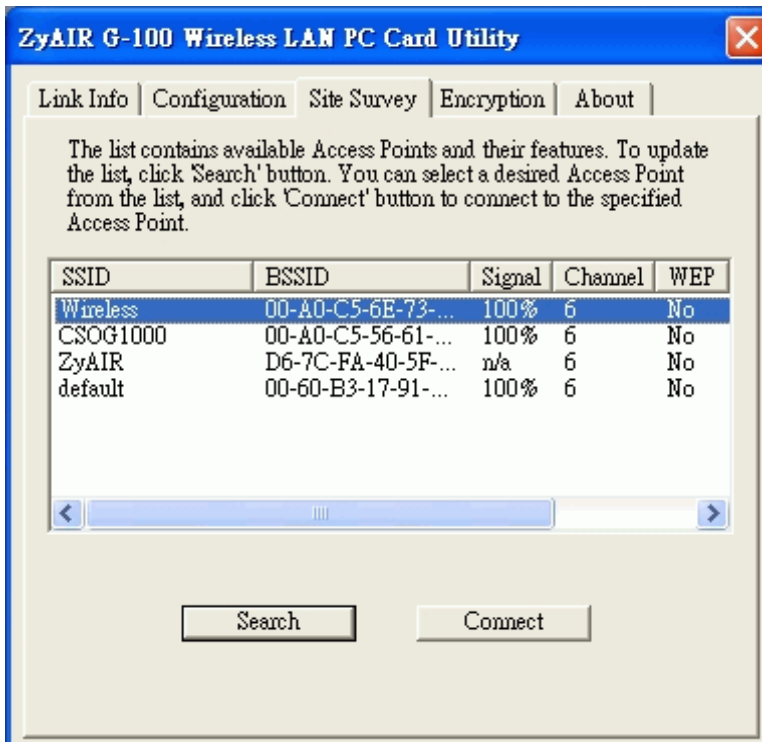
- *Configuration Wireless Station to Infrastructure mode*

To configure Infrastructure mode on your ZyAIR B-100/B-200/B-300 wireless NIC card please follow the following steps.

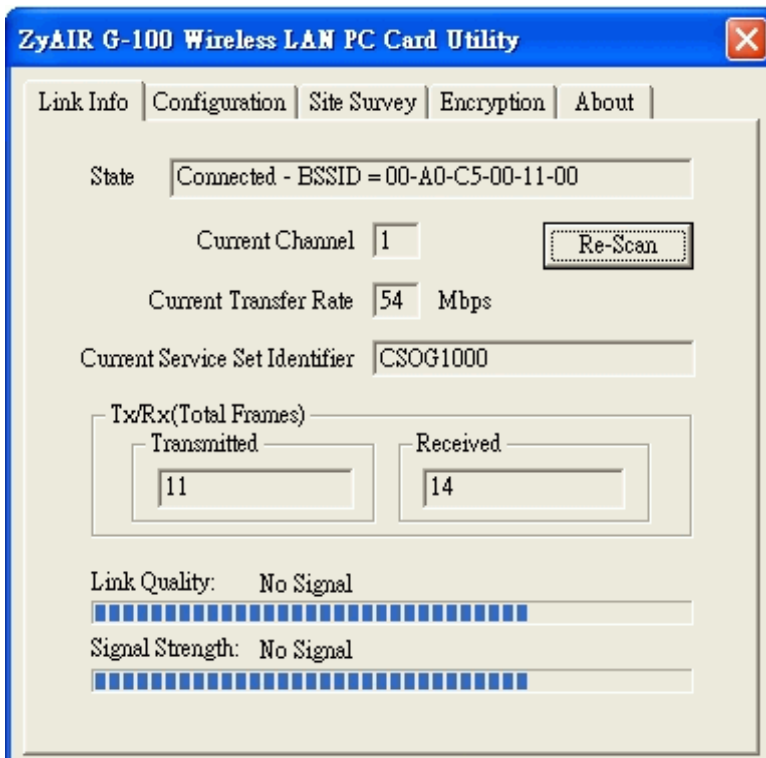
1. Double click on the utility icon in your windows task bar the utility will pop up on your windows screen.
2. Select configuration tab.



3. Select Infrastructure from the operation mode pull down menu, fill in an SSID or leave it as any if you wish to connect to any AP than press Apply Change to take effect.
4. Click on Site Survey tab, and press search all the available AP will be listed.



5. Double click on the AP you want to associated with.

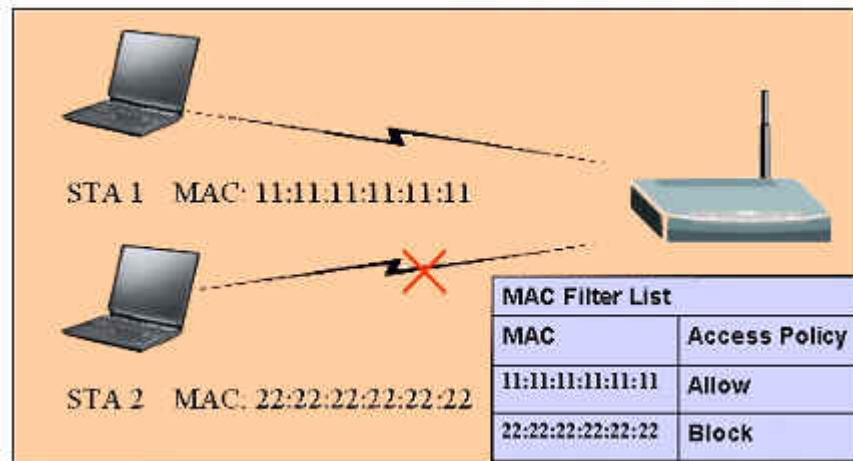


6. After the client have associated with the selected AP. The linked AP's channel, current linkup rate, SSID, link quality, and signal strength will show on the Link Info page. You now successfully associate with the selected AP with Infrastructure Mode.

## Wireless MAC address filtering

### *MAC Filter Overview*

Users can use MAC Filter as a method to restrict unauthorized stations from accessing the APs. ZyXEL's APs provide the capability for checking MAC address of the station before allowing it to connect to the network. This provides an additional layer of control layer in that only stations with registered MAC addresses can connect. This approach requires that the list of MAC addresses be configured.



---

### *2. ZyXEL MAC Filter Implementation*

ZyXEL's MAC Filter Implementation allows users to define a list to allow or block association from STAs. The filter set allows users to input 12 entries in the list. If Allow Association is selected, all other STAs which are not on the list will be denied. Otherwise, if Deny Association is selected, all other STAs which are not on the list will be allowed for association. Users can choose either way to configure their filter rule.

---

### *3. Configure the WLAN MAC Filter*

The MAC Filter related settings in ZyXEL APs are configured in menu 3.5.1, WLAN MAC Address Filter Configuration. Before you configure the MAC filter, you need to know the MAC address of the client first. If

not knowing what your MAC address is, please enter a command "ipconfig /all" after DOS prompt to get the MAC (physical) address of your wireless client.

If you use SMT management, the MAC Address Filter configuration are as shown below.

Enter the MAC Addresses of wireless cards in the filter set to allow or deny association from these cards.

```

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:
    
```

Key Settings:

Option	Descriptions
<b>Filter Action</b>	Allow or block association from MAC addresses contained in this list. If <b>Allow Association</b> is selected in this field, hosts with MAC addresses configured in this list will be allowed to associate with AP. If <b>Deny Association</b> is selected in this field, hosts with MAC addresses configured in this list will be blocked.

MAC Address	This field specifies those MAC Addresses that you want to add in the list.
-------------	--

If you use WEB configuration, the MAC Address Filter configuration are as shown below.

1. Using a web browser, login AP by giving the LAN IP address of AP in URL field. Default LAN IP is 192.168.1.1, default password to login web configurator is 1234.
2. Click **Network**, and click **Wireless LAN** tab on the left.
3. Click **MAC Filter** link and check **Active MAC Filter** to enable MAC Filter.
4. Select the **Filter Action** to allow or deny association from hosts in the list.
5. Enter the MAC Addresses which you may want to apply the filter to allow or block associations from.
6. Click **Apply** to make your setting work.

Network > Wireless LAN > MAC Filter

Active MAC Filter

Filter Action  Allow  Deny

Set	MAC Address	Set	MAC Address
1	11:11:11:11:11:11	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:00	10	00:00:00:00:00:00
11	00:00:00:00:00:00	12	00:00:00:00:00:00
13	00:00:00:00:00:00	14	00:00:00:00:00:00
15	00:00:00:00:00:00	16	00:00:00:00:00:00
17	00:00:00:00:00:00	18	00:00:00:00:00:00
19	00:00:00:00:00:00	20	00:00:00:00:00:00
21	00:00:00:00:00:00	22	00:00:00:00:00:00
23	00:00:00:00:00:00	24	00:00:00:00:00:00
25	00:00:00:00:00:00	26	00:00:00:00:00:00
27	00:00:00:00:00:00	28	00:00:00:00:00:00
29	00:00:00:00:00:00	30	00:00:00:00:00:00
31	00:00:00:00:00:00	32	00:00:00:00:00:00

Apply Cancel

## WEP configuration (Wired Equivalent Privacy)

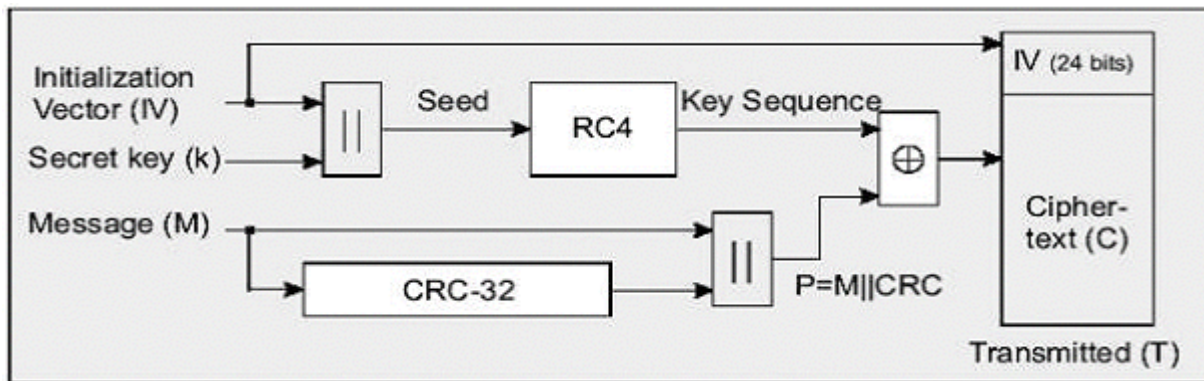
### Introduction

The 802.11 standard describes the communication that occurs in wireless LANs.

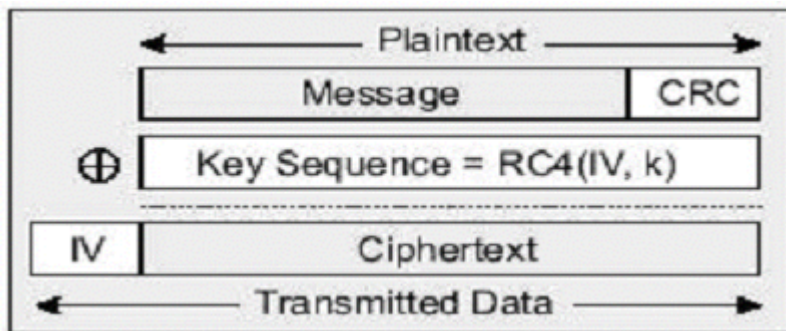
The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping, because wireless transmissions are easier to intercept than transmissions over wired networks, and wireless is a shared medium, everything that is transmitted or received over a wireless network can be intercepted.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packages are not modified during the transition. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points APs.

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



WEP has defences against this attack. To avoid encrypting two cipher texts with the same key stream, an Initialisation Vector (IV) is used to augment the shared WEP key (secret key) and produce a different RC4 key for each packet, the IV is also included in the package. WEP key (secret key) are available in two types, 64-bits and 128-bits. Many times you will see them referenced as 40-bits and 104-bits instead. The reason for this misnomer is that the WEP key (40/104 bits) is concatenated with the initialisation vector (24 bits) resulting in a 64/128 bit total key size.



### *Setting up the Access Point*



Most access points and clients have the ability to hold up to 4 WEP keys simultaneously. You need to specify one of the 4 keys as default Key for data encryption. To set up the Access Point, you will need to set the one of the following parameters:

- 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 set up the Access Point by SMT or Web configurator

- Setting up the Access Point from SMT Menu 3.5

B1000 hold up to 4 WEP Keys. You have to specify one of the 4 keys as default Key which be used to encrypt wireless data transmission.

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
  
```

### Key settings

Hexadecimal digits have to preceded by '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= 0x123456789A Key2= 0x23456789AB



	Key3= 0x3456789ABC Key4= 0x456789ABCD
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= 0x112233445566778899AABBCCDEF Key2= 0x2233445566778899AABBCCDDEE Key3= 0x3344556677889900AABBCCDDFF Key4= 0x44556677889900AABBCCDDEEFF

Select one of the WEP key as default Key to encrypt wireless data transmission. The receiver will use the corresponding key to decrypt the data.

For example, if access point use Key 3 to encrypt data, then station will use Key 3 to decrypt data. So, the Key 3 of station has to equal to the Key 3 of access point.

Though access point use Key 3 as default key, but the station can use the other Key as its default key to encrypt wireless data transmission.

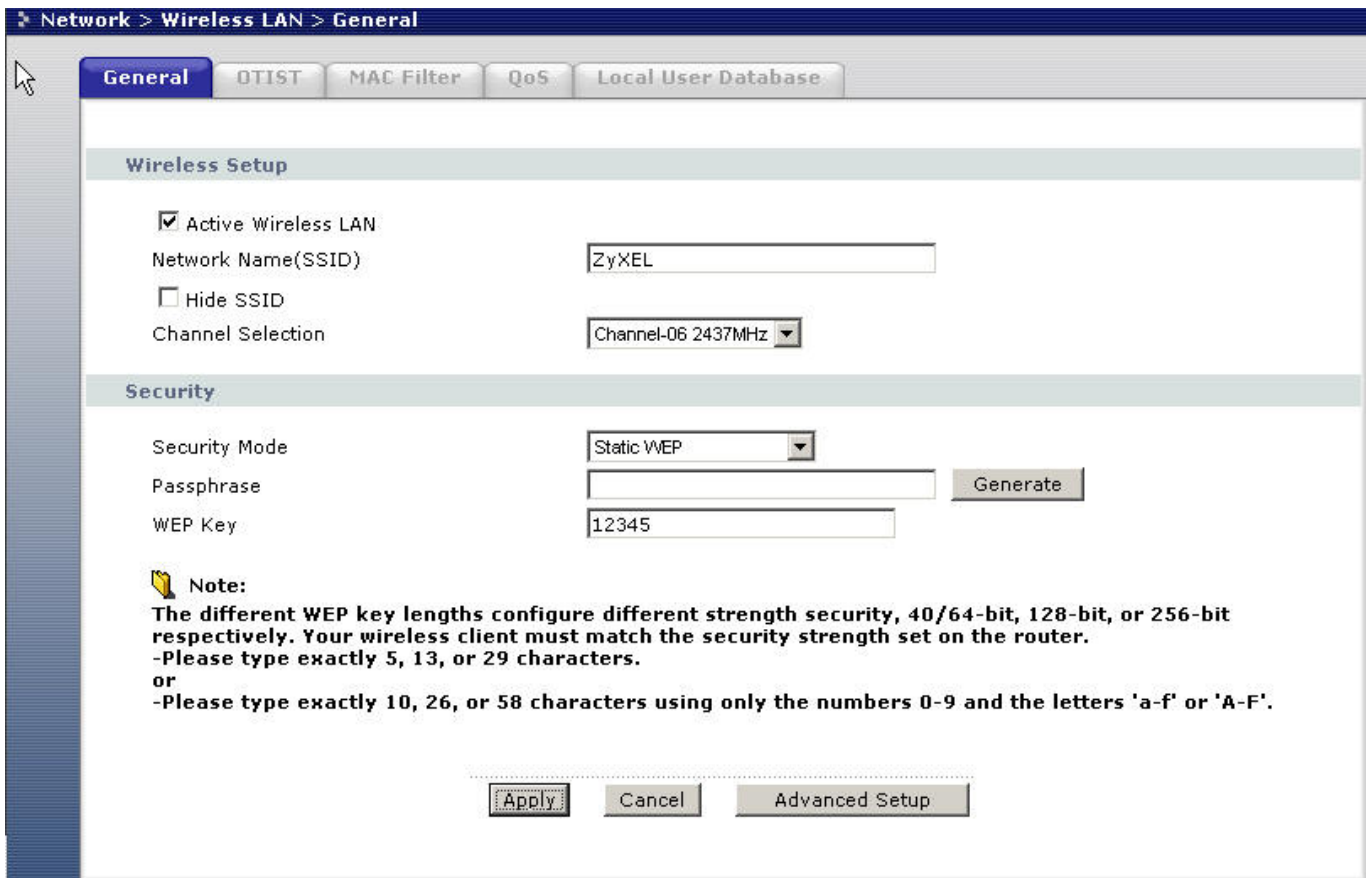
**Access Point (encrypt data by Key 3) -----> Station (decrypt data by Key 3)**

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

In this case, access point transmits data to station which encrypt data by Key 3 of access point. The station will decrypt the data by its Key 3.

At the same time, when the station transmits data to access point which encrypt data by Key 2. The access point will decrypt the data by its Key 2.

- Setting up the Access Point with Web configurator



**Key settings**

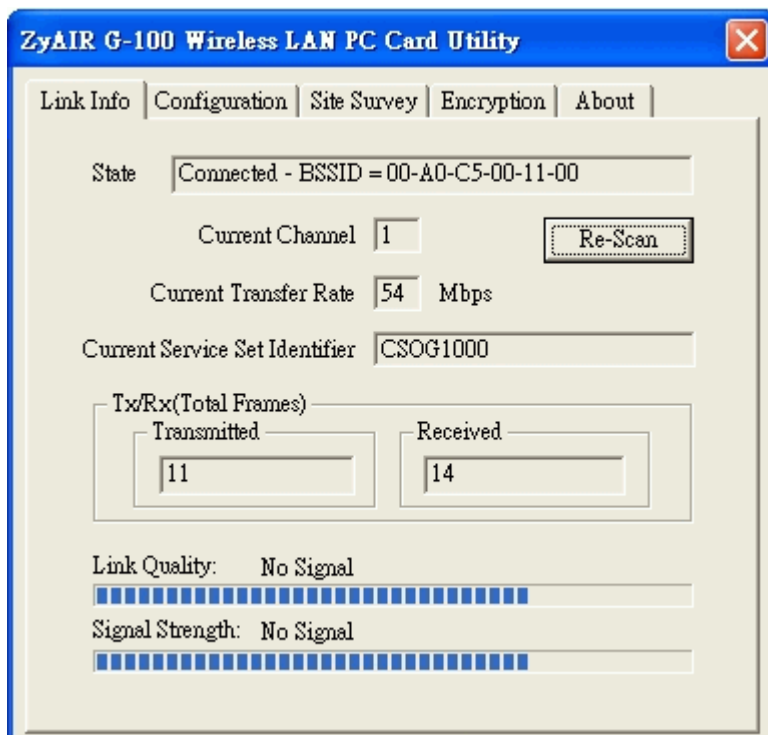
Enter exactly 5, 13 or 29 characters to match the security strength 40/64bit, 128-bit, 256-bit respectively.

**Setting up the Station**

1. Double click on the utility icon in your windows task bar or right click the utility icon then select 'Show Config Utility'.



The utility will pop up on your windows screen.



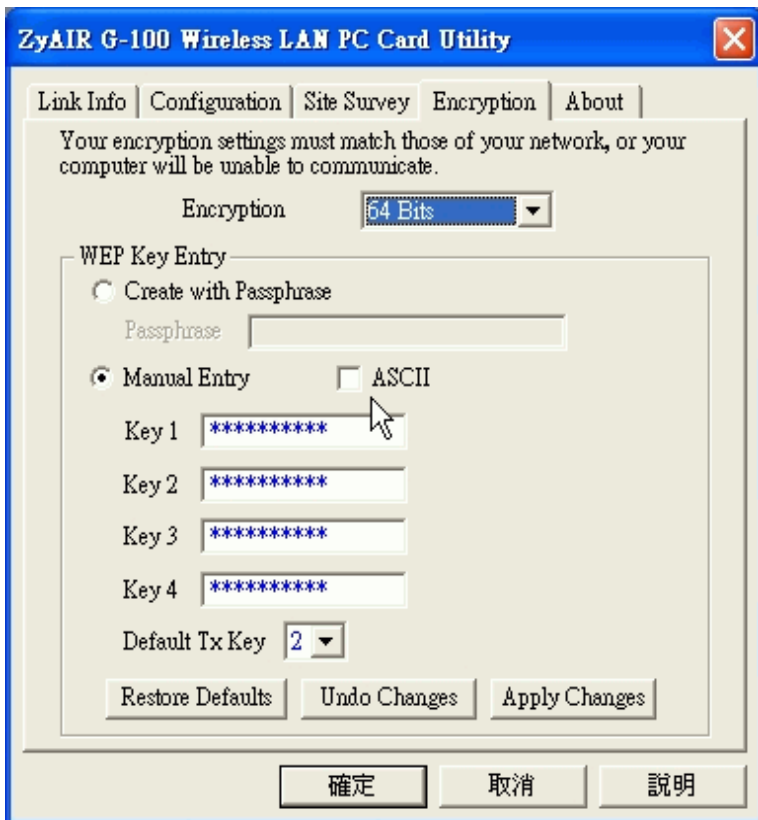
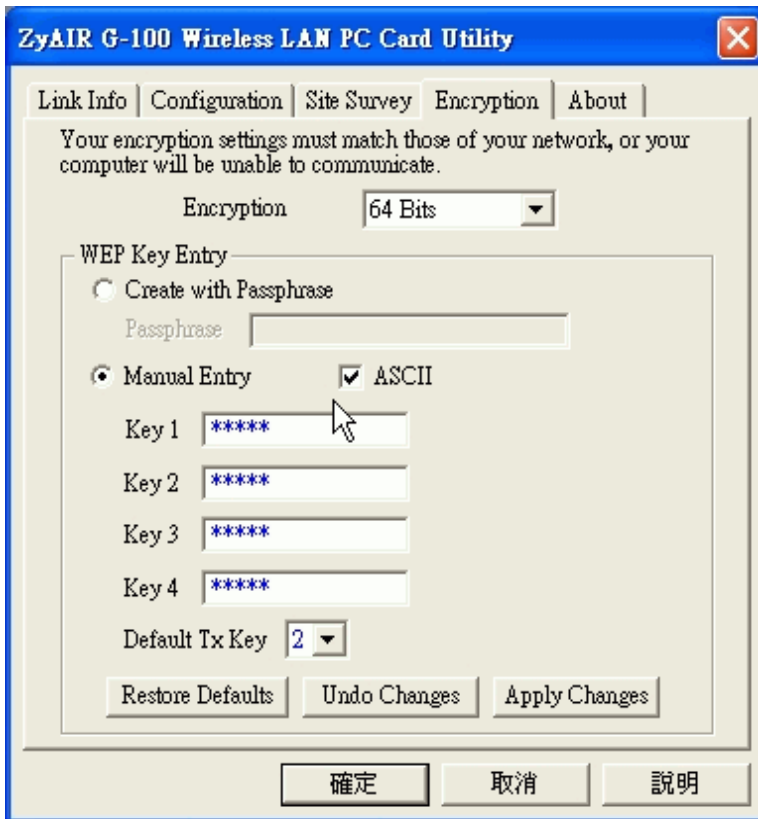
Note: If the utility icon doesn't exist in your task bar, click Start -> Programs -> IEEE802.11b WLAN Card -> IEEE802.11b WLAN Card.

2. Select the 'Encryption' tab.

Select encryption type correspond with access point.

Set up 4 Keys which correspond with the WEP Keys of access point.

And select on WEP key as default key to encrypt wireless data transmission.



### Key settings

The WEP Encryption type of station has to equal to the access point.

**Check 'ASCII'** field for characters WEP key or **uncheck 'ASCII'** field for Hexadecimal digits WEP key. Hexadecimal digits don't need to be preceded by '0x'.

For example,

64-bits with characters WEP key :

Key1= 2e3f4

Key2= 5y7js

Key3= 24fg7

Key4= 98jui

64-bits with hexadecimal digits WEP key :

Key1= 123456789A

Key2= 23456789AB

Key3= 3456789ABC

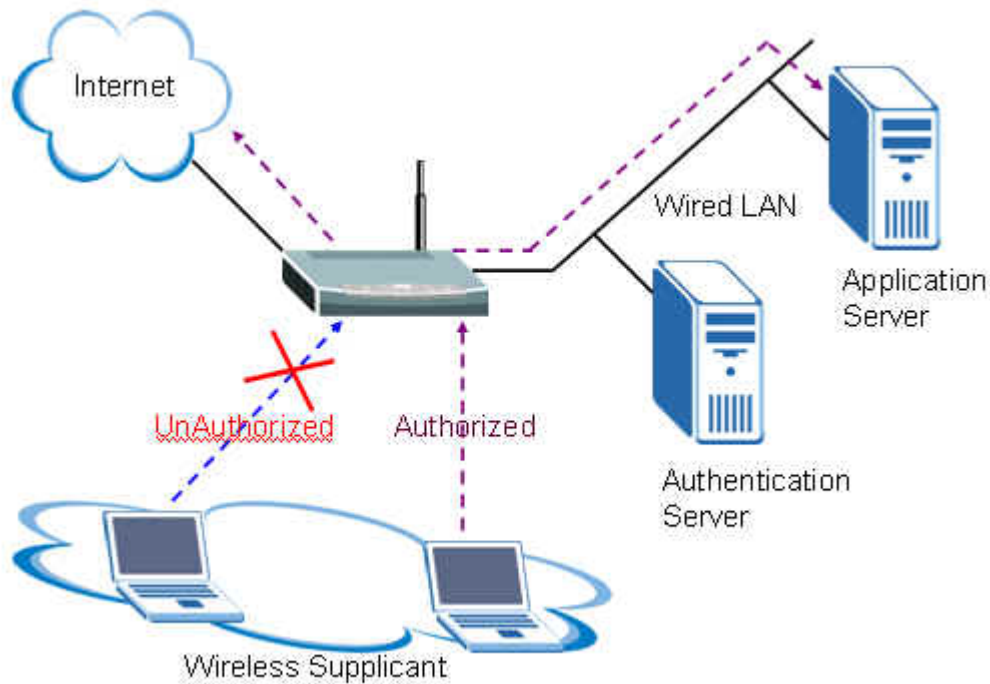
Key4= 456789ABCD

---

## Configuring 802.1x

### *IEEE 802.1x Introduction*

IEEE 802.1x port-based authentication is desired to prevent unauthorized devices (clients) from gaining access to the network. As LANs extend to hotels, airports, and corporate lobbies, insecure environments could be created. 802.1x port-based network access control makes use of the physical access characteristics of **IEEE 802 LAN infrastructures**, such as 802.3 Ethernet, 802.11 Wireless LAN and VDSL LRE (Long Reach Ethernet), in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases the authentication process fails.



IEEE 802.1x authentication is a client-server architecture delivered with EAPOL (Extensible Authentication Protocol over LAN). The authentication server authenticates each client connected to a Access Point (For Wireless LAN) or switch port (for Ethernet) before accessing any services offered by the Wireless AP. 802.1x contains three major components :

### 1. Authenticator :

The device (i.e. Wireless AP) facilitates authentication for the supplicant (Wireless client) attached on the Wireless network. Authenticator controls the physical access to the network based on the authentication status of the client. The authenticator acts as an intermediary (proxy) between the client and the authentication server (i.e. RADIUS server), requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

### 2. Supplicant :

The station (i.e. Wireless client) is being authenticated by an authenticator attached on the Wireless network. The supplicant requests access to the LAN services and responds to the requests from the authenticator. The station must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system, Meeting House AEGIS 802.1x client and Odyssey 802.1x client.

### 3. Authentication Server :

The device (i.e. RADIUS server) provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator. The authentication server performs the actual authentication of the client. It validates the identity of the supplicant. Because the authenticator acts as the proxy, the authentication service is transparent to the supplicant.

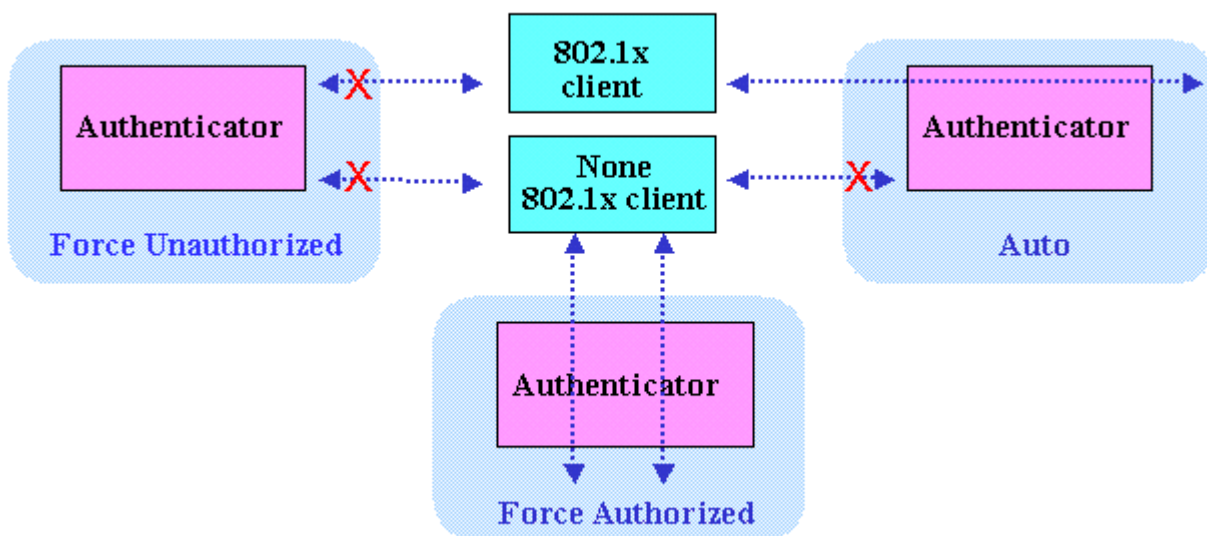
Some Wireless AP (i.e. ZyXEL Wireless AP) have built-in authentication server, external RADIUS authentication server is not needed. In this case, Wireless AP is acted as both authenticator and authentication server.

- **Authentication Port State and Authentication Control**

The port state determines whether or not the supplicant (Wireless Client) is granted access to the network behind Wireless AP. There are two authentication port state on the AP, **authorized state** and **unauthorized state**.

By default, the port starts in the unauthorized state. While in this state, the port disallows all incoming and outgoing data traffic except for 802.1x packets. When a supplicant is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally. If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the authenticator requests the client's identity. In this situation, the client does not respond to the 802.1x request, the port remains in the unauthorized state, and the client is not granted access to the network.

When 802.1x is enabled, the authenticator controls the port authorization state by using the following control parameters. The following three authentication control parameter are applied in Wireless AP.



1. **Force Authorized** : Disables 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 802.1x-based authentication of the client. This is the default port control setting. While AP is setup as **Force Authorized**, Wireless client (supported 802.1x client or none-802.1x client) can always access the network.
2. **Force Unauthorized** : Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The authenticator cannot provide authentication services to the supplicants through the port. While AP is setup as **Force Unauthorized**, Wireless clients (supported 802.1x client or none-802.1x client) never have the access for the network.
3. **Auto** : Enables 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 requests the identity of the client and begins relaying authentication messages between supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the authenticator by using the client's MAC address. While AP is setup as **Auto**, only Wireless client supported 802.1x client can access the network.

- ***Re-Authentication***

The administrator can enable periodic 802.1x client re-authentication and specify how often it occurs. When re-authentication time out, Authenticator will send EAP-Request/ Identity to reinitiate authentication process. In ZyXEL Wireless AP 802.1x implementation, if you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 1800 seconds (30 minutes).

- ***EAPOL (Extensible Authentication Protocol over LAN)***

Authenticators and supplicants communicate with one another by using the Extensible Authentication Protocol (EAP, RFC-2284). EAP was originally designed to run over PPP and to authenticate dial-in users, but 802.1x defines an encapsulation method for passing EAP packets over Ethernet frames. This method is referred to as **EAP over LANs, or EAPOL**. Ethernet type of EAPOL is **88-8E**, two octets in length. EAPOL encapsulations are described for IEEE 802 compliant environment, such as 802.3 Ethernet, 802.11 Wireless LAN and Token Ring/FDDI.



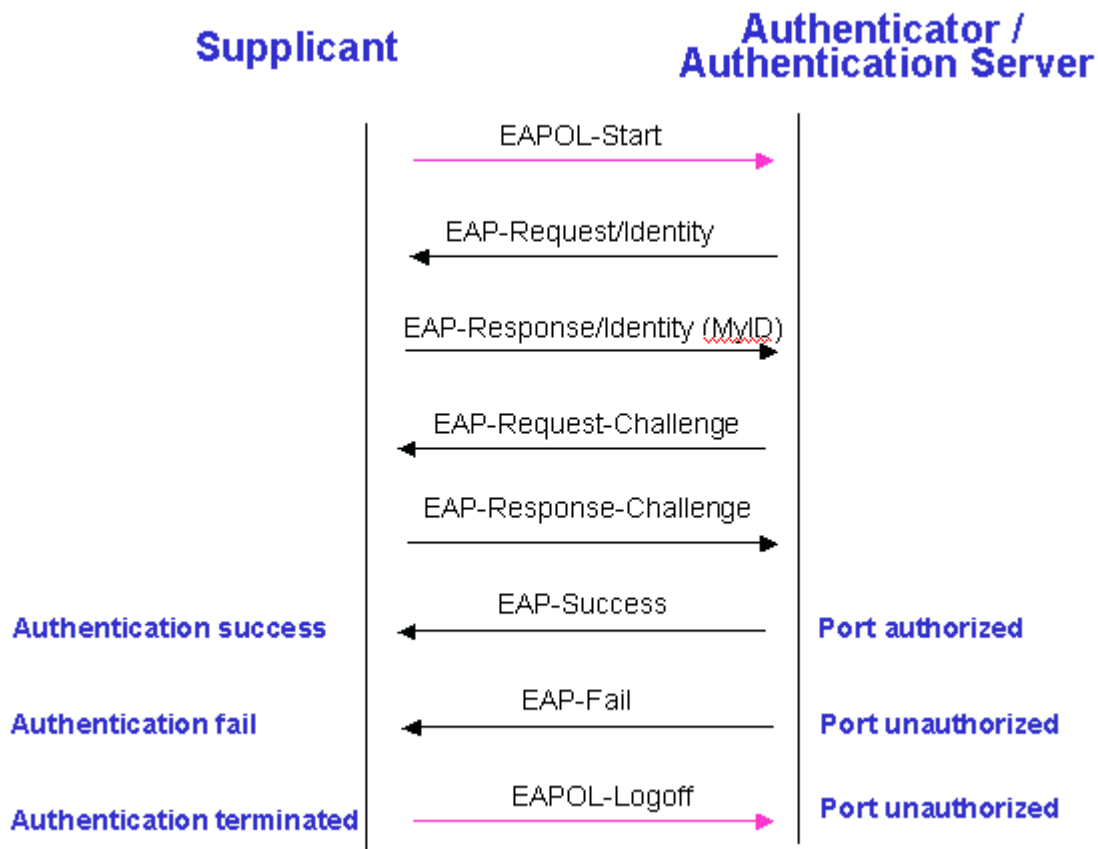


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When supplicant receive the EAP request, it will reply associated EAP response. So far, ZyXEL Wireless AP only supports MD-5 challenge authentication mechanism, but will support TLS and TTLS in the future.

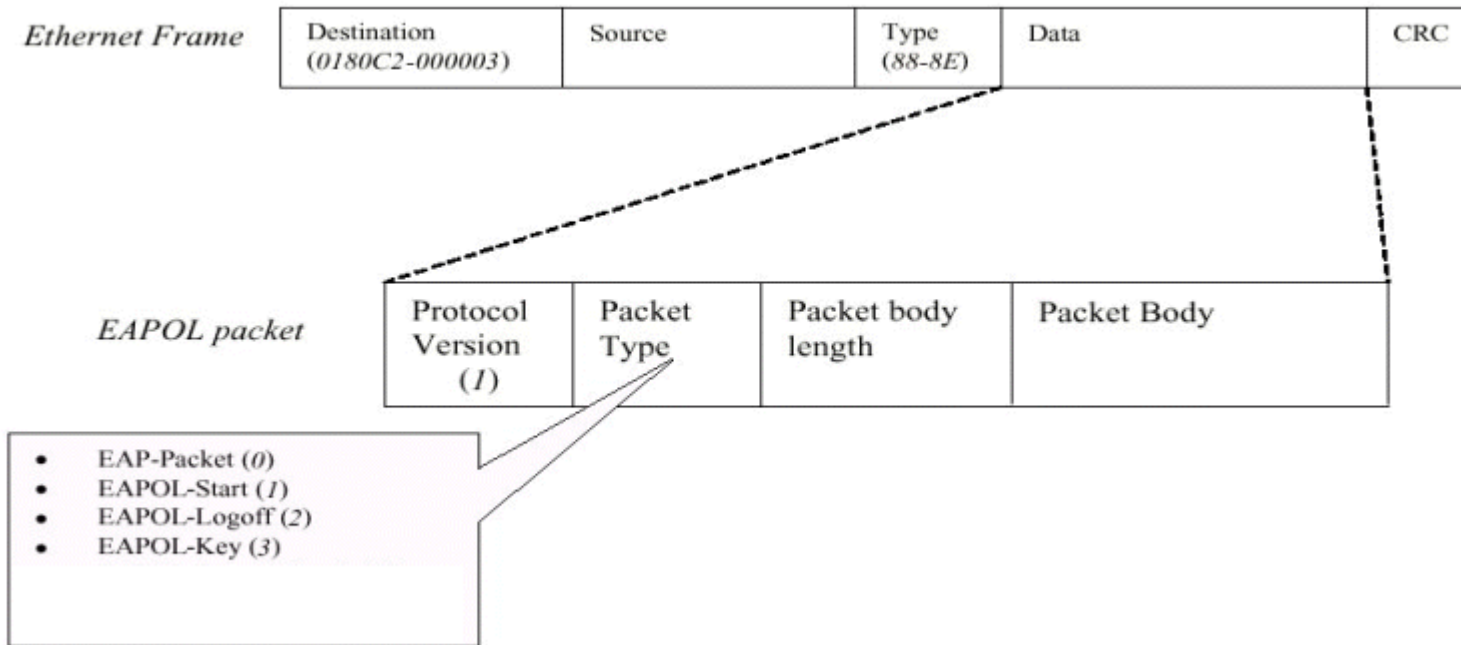
#### **EAPOL Exchange between 802.1x Authenticator and Supplicant**

The authenticator or the supplicant can initiate authentication. If you enable 802.1x authentication on the Wireless AP, the authenticator must initiate authentication when it determines that the Wireless link state transitions from down to up. It then sends an EAP-request/identity frame to the 802.1x client to request its identity (typically, the authenticator sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the supplicant responds with an EAP-response/identity frame.

However, if during bootup, the supplicant does not receive an EAP-request/identity frame from the Wireless AP, the client can initiate authentication by sending an **EAPOL-Start** frame, which prompts the switch to request the supplicant's identity. In above case, authenticator co-locate with authentication server. When the supplicant supplies its identity, the authenticator directly exchanges EAPOL to the supplicant until authentication succeeds or fails. If the authentication succeeds, the port becomes authorized. If the authentication fails, the port becomes unauthorized. When the supplicant does not need Wireless access any more, it sends **EAPOL-Logoff** packet to terminate its 802.1x session, the port state will become unauthorized. The following figure shows the EAPOL exchange ping-pong chart.



The EAPOL packet contains the following fields: protocol version, packet type, packet body length and packet body. Most of the fields are obvious. The packet type can have four different values, and these values are described below:



- EAP-Packet : Both the supplicant and the authenticator send this packet when authentication is taking place. This is the packet that contains either the MD5-Challenge or TLS information required for authentication.
- EAPOL-Start : This supplicant sends this packet when it wants to initiate the authentication process.
- EAPOL-Logoff : The supplicant sends this packet when it wants to terminate its 802.1x session.
- EAPOL-Key : This is used for TLS authentication method. The Wireless AP uses this packet to send the calculated WEP key to the supplicant after TLS negotiation has completed between the supplicant and the RADIUS server.

---

**IEEE 802.1x Configuration in ZyXEL Wireless Access Point**

- **Enable 802.1x in AP**

When the IEEE 802.1x authentication is enabled, the wireless client must be authenticated by the ZyXEL AP before it can communicate on your network through ZyXEL AP. By default, the 802.1x function is disabled (Authentication Control= Force Authorized) to allow all wireless client. You can use SMT or Web Configuration to configure it.

Enter SMT Menu 23.4 to setup the 802.1x authentication control.

Menu 23.4 - System Security - IEEE802.1x

Wireless Port Control= **No Authentication Required**

ReAuthentication Timer (in second)= N/A

Idle Timeout (in second)= N/A

Key Management Protocol= N/A

Dynamic WEP Key Exchange= N/A

PSK= N/A

WPA Mixed Mode= N/A

Data Privacy for Broadcast/Multicast packets= N/A

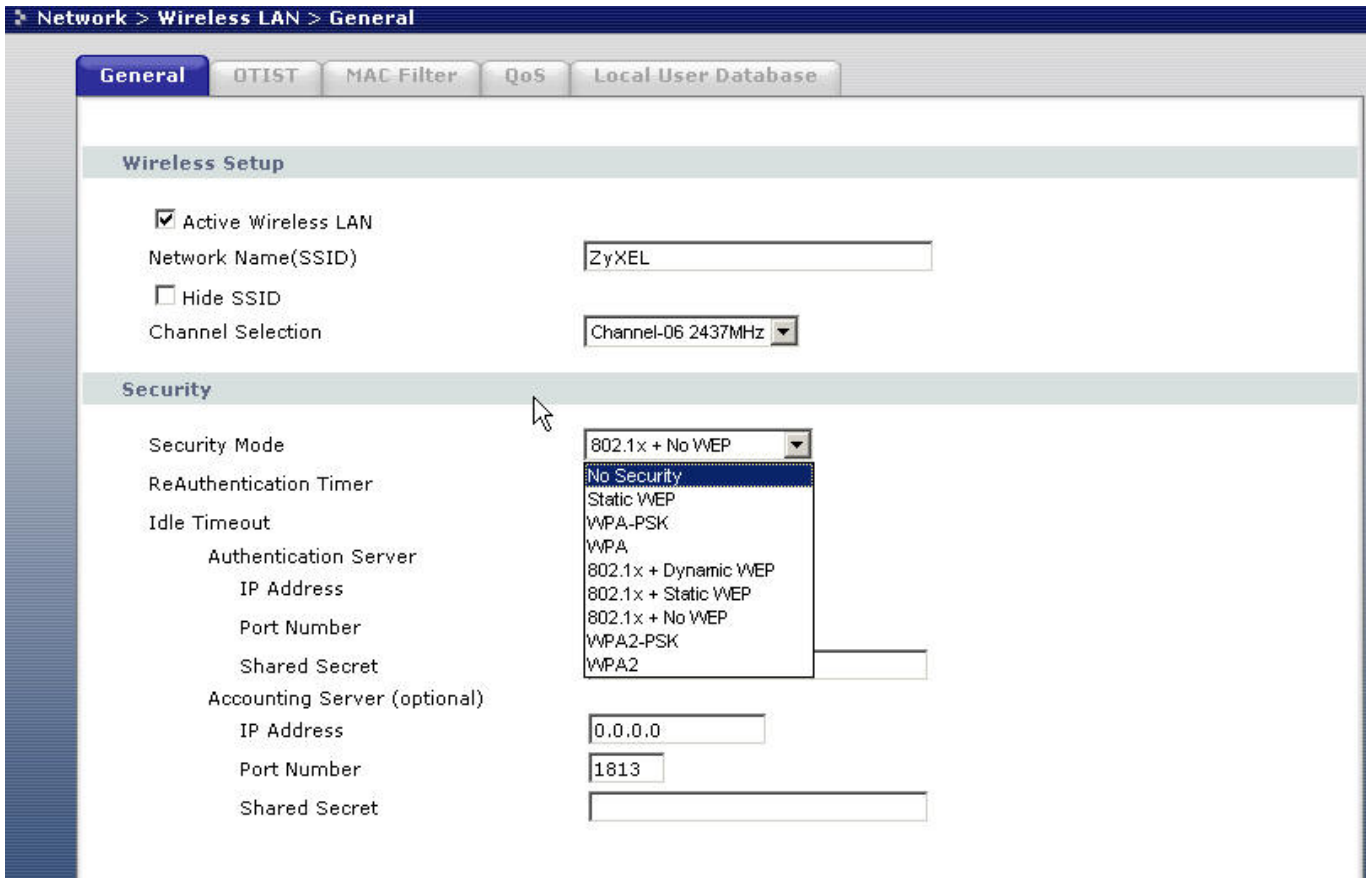
WPA Broadcast/Multicast Key Update Timer= N/A

Authentication Databases= N/A

Press ENTER to Confirm or ESC to Cancel:

If you use WEB Configuration,

1. From the Web Configurator main menu, Click Network -> Wireless LAN -> and select 802.1x
2. Click **Apply** to make your setting work.



- *Using Internal Authentication Server*

ZyXEL Wireless Access Point has an internal authentication server for authenticating the wireless 802.1x client users. It builds total 32-users database and allows up to 32 authorized users to login to the Wireless AP simultaneously. When you use internal authentication server, ZyXEL wireless AP is acted as Authenticator and Authentication Server.

By storing wireless 802.1x client profiles locally, your ZyXEL AP is able to authenticate wireless client without interacting with a extra network RADIUS server. Follow the steps to add user accounts on your ZyXEL AP.

1. From the SMT main menu, enter 14 to display Menu 14 Dial-in User Setup

**Menu 14 - Dial-in User Setup**

1. ZyXEL      9. \_\_\_\_\_      17. \_\_\_\_\_      25. \_\_\_\_\_

2. _____	10. _____	18. _____	26. _____
3. _____	11. _____	19. _____	27. _____
4. _____	12. _____	20. _____	28. _____
5. _____	13. _____	21. _____	29. _____
6. _____	14. _____	22. _____	30. _____
7. _____	15. _____	23. _____	31. _____
8. _____	16. _____	24. _____	32. _____

Enter Menu Selection Number:

2. Type a number and press [Enter] to edit the wireless 802.1x client profile

Menu 14.1 - Edit Dial-in User

User Name= **ZyXEL**

Active= **Yes**

Password= **\*\*\*\*\***

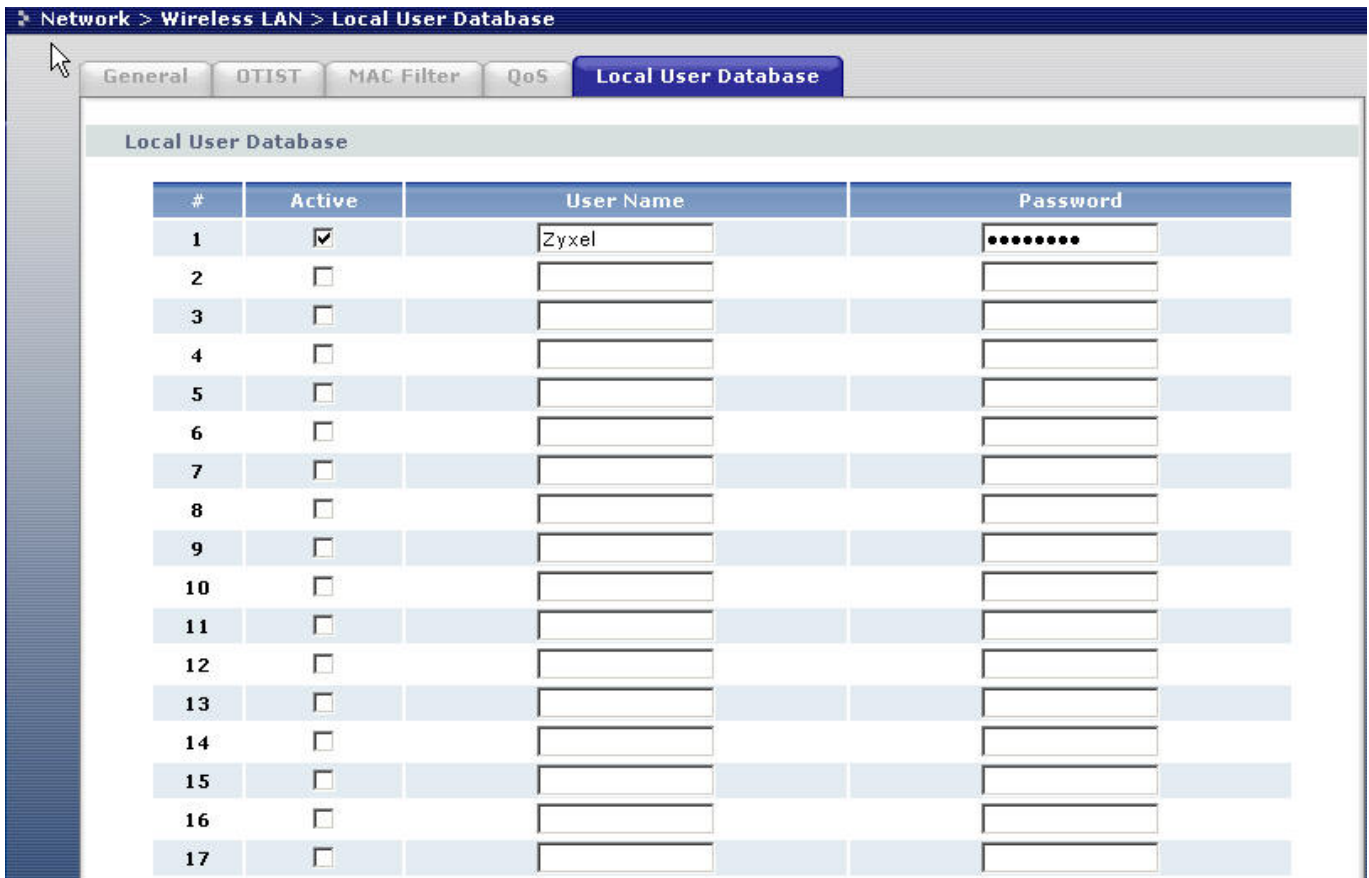
Press ENTER to Confirm or ESC to Cancel:

Key settings :

Option	Descriptions
<b>User Name</b>	Enter a username up to 31 alphanumeric characters long.
<b>Active</b>	Press [SPACE BAR] to select <b>Yes</b> and press [Enter] to activate this 802.1x client profile.
<b>Password</b>	Enter a password up to 31 characters long.

If you use WEB Configurator,

1. From the Web Configurator main menu, Network -> Wireless LAN -> Local User Database
2. Select one of the profile and check **Active** check box
3. Input the **User Name and Password** then click **Apply** to save the profile.

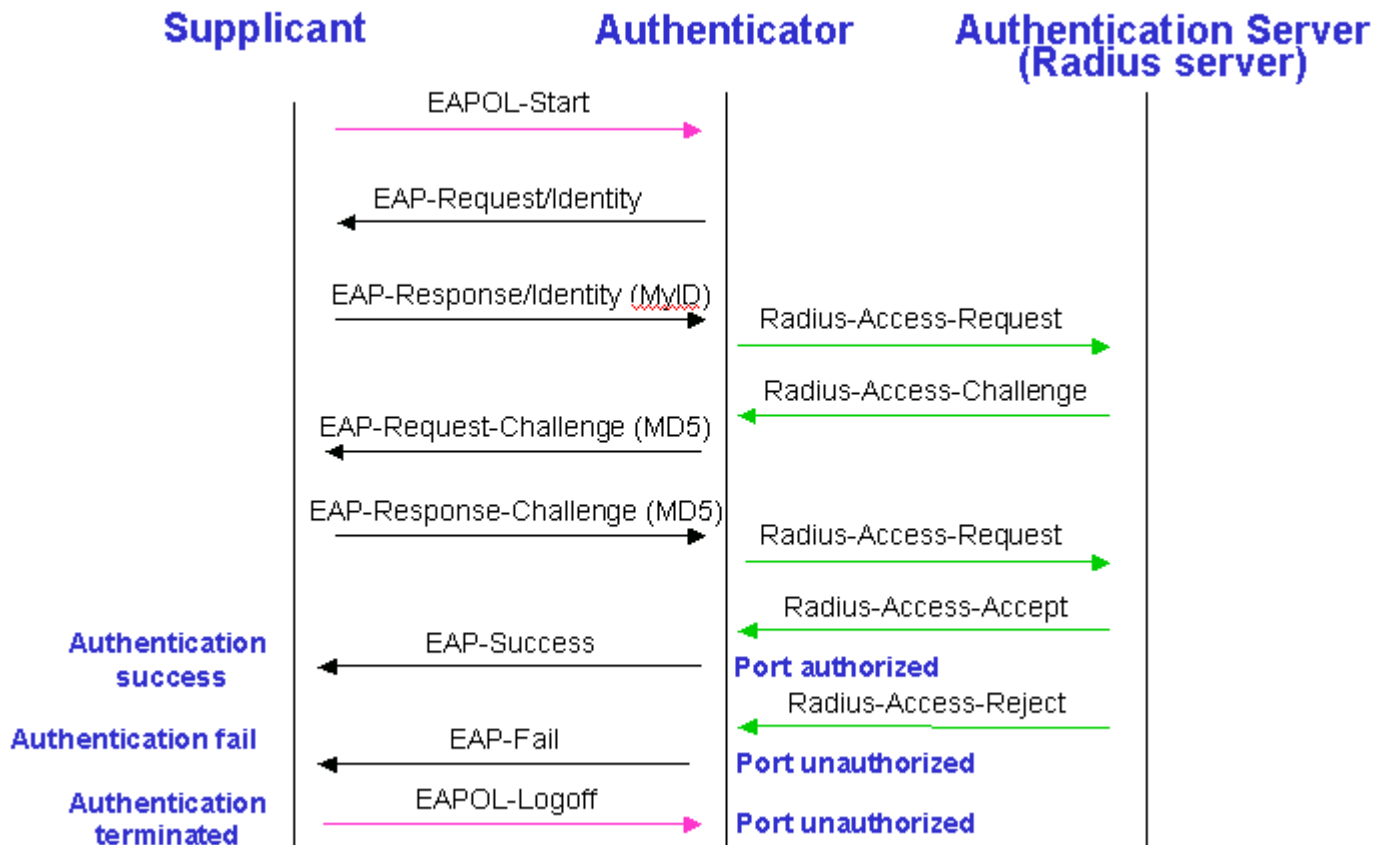


- **Using External RADIUS Authentication Server**

In addition to the internal authentication server inside ZyXEL AP, you can use external RADIUS authentication server to centrally manage the user account profile. RADIUS is based on a client-server model that supports authentication, authorization and accounting. The wireless AP is the client and the server is the RADIUS server.

The authenticator includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the authenticator receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the supplicant. When the client supplies its identity, the authenticator begins its role as the intermediary, passing EAP frames

between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. The specific exchange of EAP frames depends on the authentication method being used. The figure below shows a message exchange initiated by the client using the MD5 Challenge authentication method with a RADIUS server.



1. From the SMT main menu, enter Menu 23.2 to setup System Security - RADIUS Server to setup the RADIUS authentication server.

Menu 23.2 - System Security - RADIUS Server

Authentication Server:  
Active= **Yes**  
Server Address= **192.168.1.100**  
Port #- **1812**



Shared Secret= \*\*\*\*\*

Accounting Server:

Active= Yes

Server Address= 192.168.1.100

Port #= 1813

Shared Secret= \*\*\*\*\*

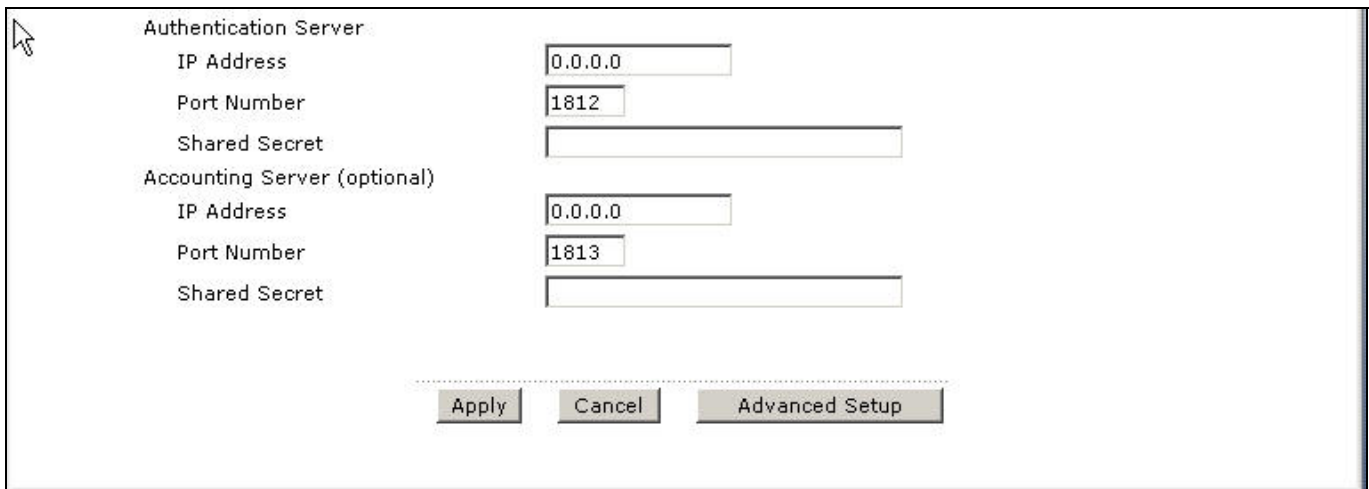
Press ENTER to Confirm or ESC to Cancel:

**Key settings for authentication server:**

Option	Descriptions
<b>User Name</b>	Enter a username up to 31 alphanumeric characters long.
<b>Active</b>	Press [SPACE BAR] to select <b>Yes</b> and press [Enter] to enable 802.1x user authentication through an external RADIUS authentication server. Select <b>No</b> to enable authentication using ZyXEL AP internal authentication server.
<b>Server Address</b>	Enter the IP address of the external RADIUS authentication server.
<b>Port</b>	The default port of RADIUS server for authentication is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so.
<b>Shared Secret</b>	Specify a password (up to 31 characters) as the key to be shared between external RADIUS authentication server and ZyXEL AP (RADIUS client). The key is not send to the network. This key must be the same on the external RADIUS authentication server and ZyXEL AP.

2. If accounting is required, you must setup the external RADIUS accounting server. Normally, RADIUS authentication server and RADIUS accounting server are put in the same machine. However, they own separated UDP port and shared secret, you can separate authentication and accounting service in two different RADIUS servers. You can refer to RADIUS authentication configuration.

If you use WEB Configurator, from the Web Configurator main menu, Click Network -> Wireless Lan to setup the RADIUS authentication and accounting server configuration.



The screenshot shows a configuration window for the ZyXEL Prestige 2602HWL-DxA. It is divided into two sections: 'Authentication Server' and 'Accounting Server (optional)'. Each section has three input fields: 'IP Address', 'Port Number', and 'Shared Secret'. The 'Authentication Server' fields are pre-filled with '0.0.0.0', '1812', and an empty field. The 'Accounting Server (optional)' fields are pre-filled with '0.0.0.0', '1813', and an empty field. At the bottom of the window, there are three buttons: 'Apply', 'Cancel', and 'Advanced Setup'.

Section	Field	Value
Authentication Server	IP Address	0.0.0.0
	Port Number	1812
	Shared Secret	
Accounting Server (optional)	IP Address	0.0.0.0
	Port Number	1813
	Shared Secret	

## Site Survey

### *Introduction*

What is Site Survey?

An RF site survey is a MAP to RF contour of RF coverage in a particular facility. With wireless system it is very difficult to predict the propagation of radio waves and detect the presence of interfering signals. Walls, doors, elevator shafts, and other obstacles offer different degree of attenuation. This will cause the RF coverage pattern be irregular and hard to predict.

Site survey can help us overcome these problem and even provide us a map of RF coverage of the facility.

### *Preparation*

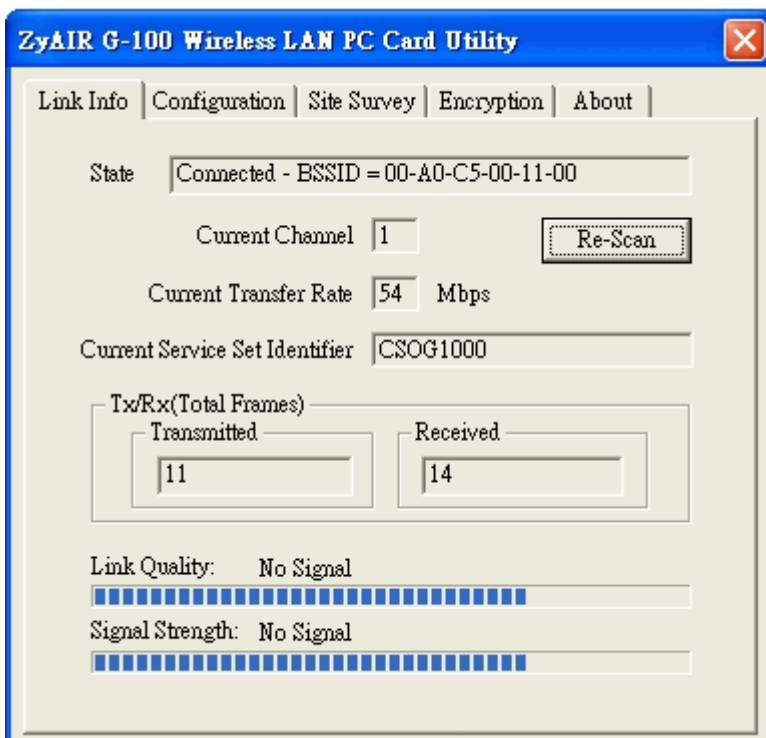
Below are the step to complete a simple site survey with simple tools.

1. First you will need to Obtain a facility diagram, such as a blueprints. This is for you to mark and take record on.
2. Visually inspect the facility, walk through the facility to verify the accuracy of the diagram and mark down any large obstacle you see that may effect the RF signal such as metal shelf, metal desk, etc on the diagram.

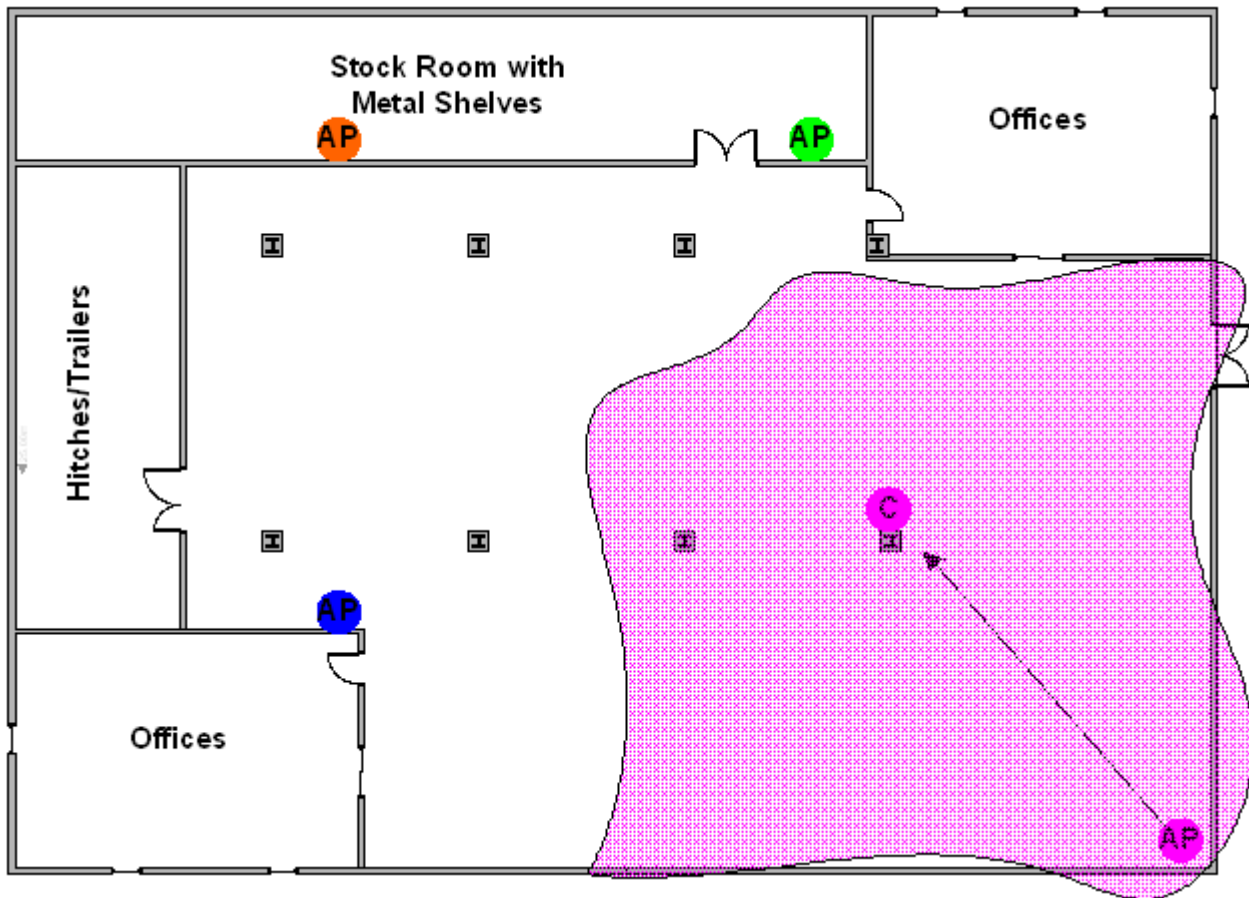
3. Identify user's area, when doing so ask a question where is wireless coverage needed and where does not, and note and take note on the diagram this is information is needed to determine the number of AP required.
4. Determine the preliminary access point location on the facility diagram base on the service area needed, obstacles, power wall jack considerations.

*Survey on Site*

1. With the diagram with all information you gathered in the preparation phase. Now you are ready to make the survey.
2. Install an access point at the preliminary location.
3. Use a notebook with wireless client installed and run it's utility. An utility will provide information such as connection speed, current used channel, associated rate, link quality, signal strength and etc information as shown in utility below.



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

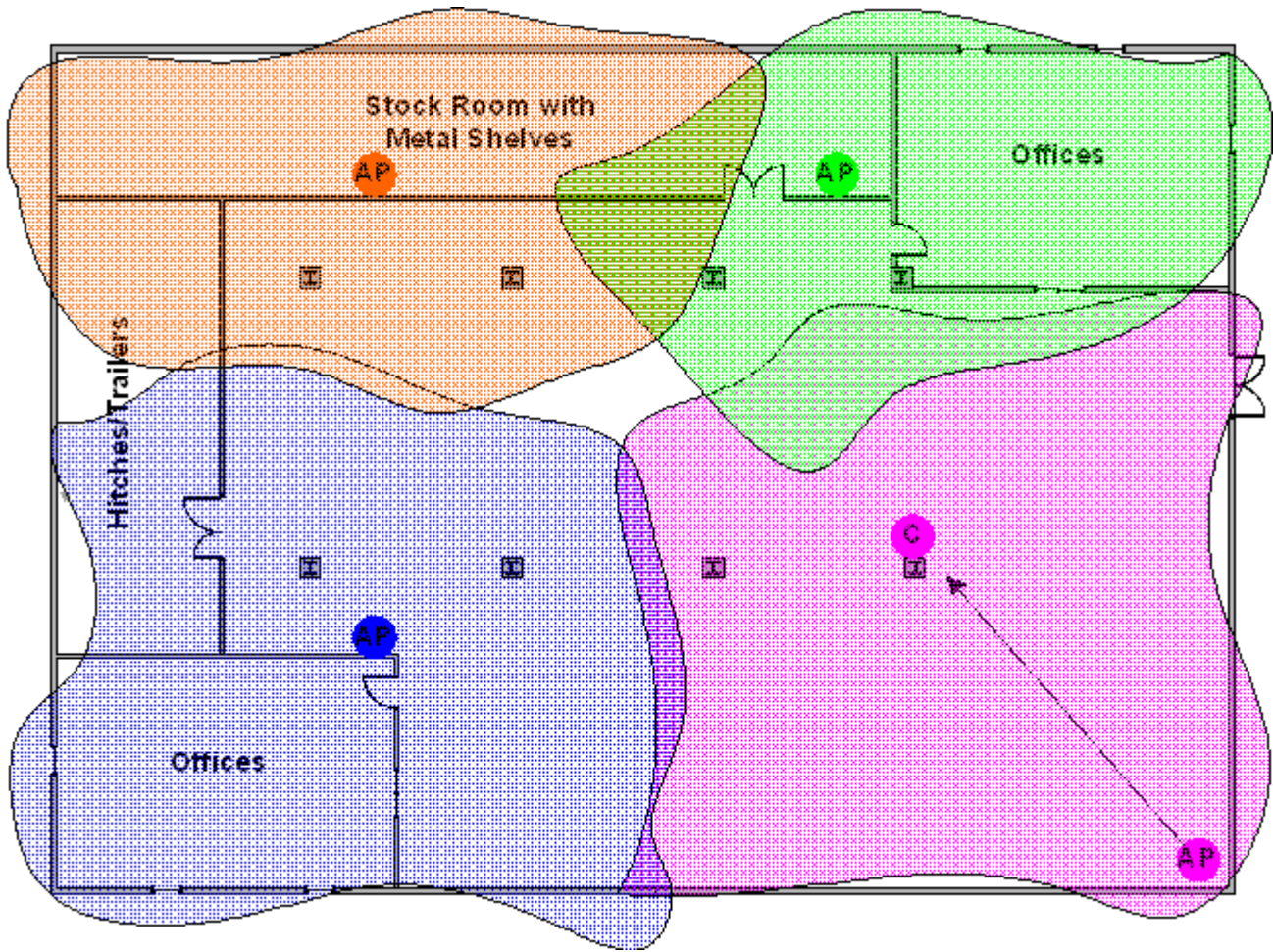


5. When you reach the farthest point of connection mark the spot. Now you move the access point to this new spot as have already determine the farthest point of the access point installation spot if wireless service is required from corner of the room.

6. Repeat step 1~5 and now you should be able to mark an RF coverage area as illustrated in above picutre.

7. You may need more than one access point is the RF coverage area have not cover all the wireless service area you needed.

8. Repeat step 1~6 of survey on site as necessary, upon completion you will have an diagram and information of site survey. As illustrated below.



Note: If there are more than one access point is needed be sure to make the adjacent access point service area over lap one another. So the wireless station are able to roam. For more information please refer to roaming at

## PSTN Lifeline Application Notes (For Lifeline model only)

### Usage of PSTN Lifeline

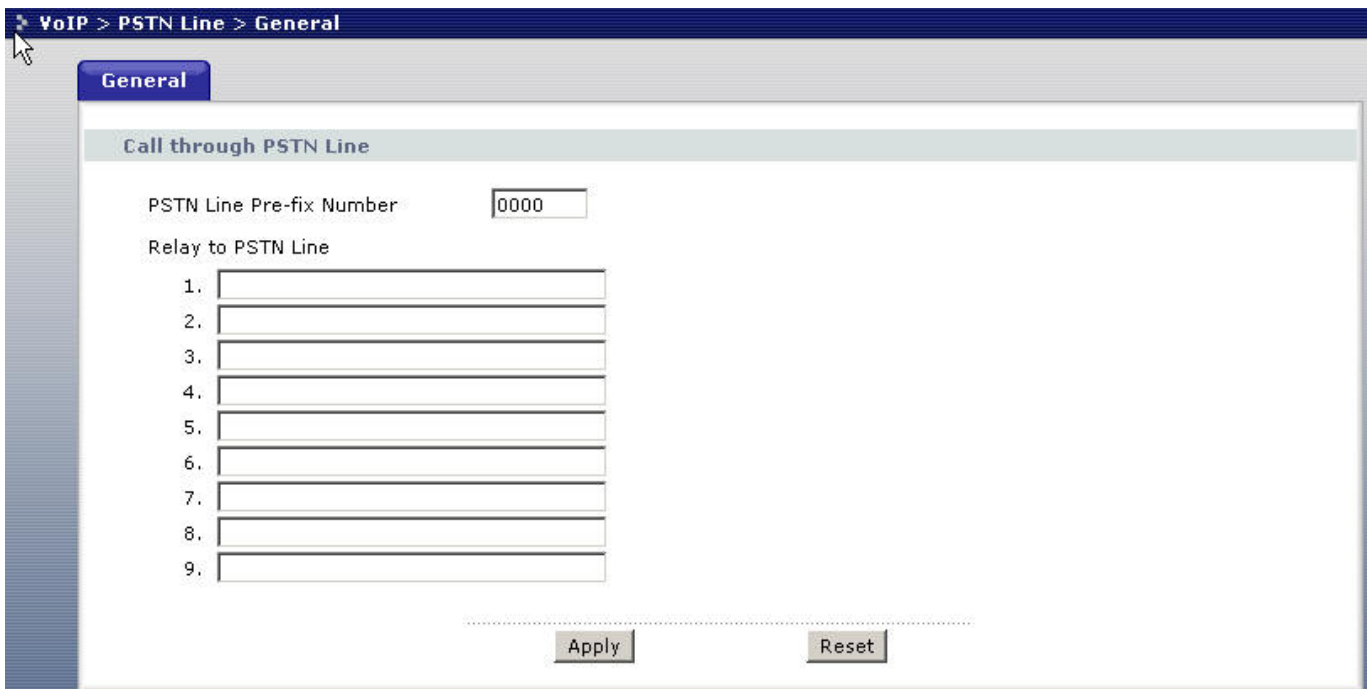
By using the PSTN lifeline function, you can make and receive regular PSTN phone calls in coexistence with VoIP service on the same set of phone. This can be done by simply assigning a prefix number (by default the prefix for PSTN dial out is 0000 and can be change to value you wish to) and dial this prefix to switch over to PSTN line than dial the PSTN number as normal.

Furthermore, when the P2602HWL – D1A experience power loss such as in case of earthquake and other natural hazard that cause power loss, it will automatically switch to PSTN line and you can dial a regular phone number without dialing a prefix number.

This can be applied on the emergency situation such as for contacting police, fire or emergency medical services when is powerless situation. On the following section, it tells you how to configure lifeline under P2602HWL – D1A WEB GUI.

**Lifeline configuration**

To configure lifeline in P2602HWL – D1A, click on VoIP -> PSTN Line to display the following screen.



You can specify a prefix number in prefix field. This number will be used to switch from VoIP to PSTN system when you wish to make a call to PSTN destination. For example, when you want to dial out to a PSTN destination, you first pick up the phone, and you will heard a dial tone, than you push in the prefix number as defined in prefix field in this case it will be 0000, than the device will switch over to PSTN line. At this moment you will heard dial tone from PSTN again. At this state 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, P2602HWL - D1A support up to nine entries under this field.

After configuring the PSTN setup, click “Apply” to save changes back to P2602HWL - D1A.

Note: It is recommended to configure your local emergency services such as Police Dept, Fire Dept, 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 P2602HWL-D1A’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 2 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.

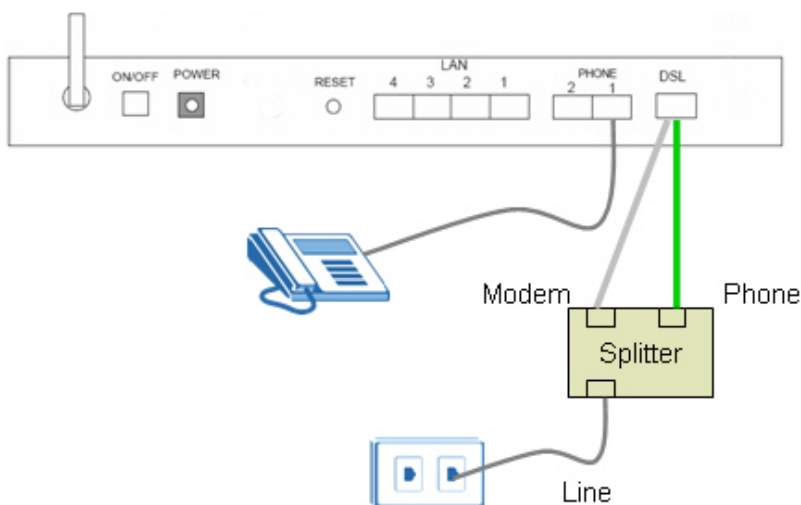


Figure 1 Splitter type

1. The P2602HWL-D1A 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 label **Line** to ADSL line from the ISP.

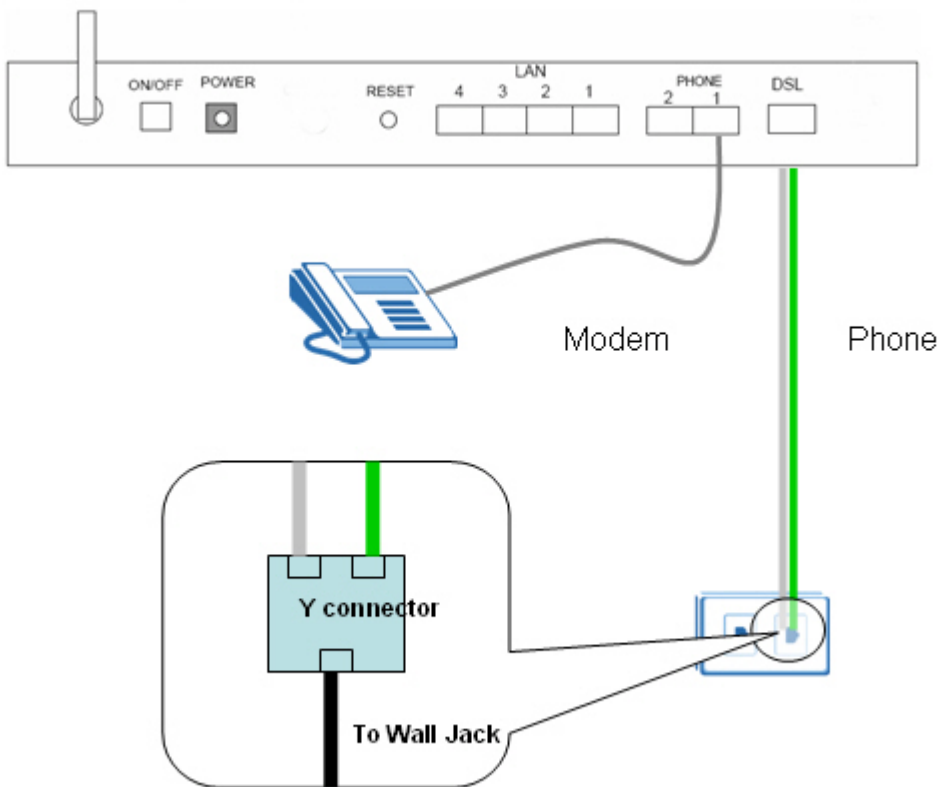


Figure 2 Splitterless type

1. The P2602HWL-D1A 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



### Setup SIP Account

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

The 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 can hold up to two SIP account simultaneously please follow the below instruction to configure the SIP account properly.

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

VoIP > SIP > SIP Settings

SIP Settings QoS

SIP Account : SIP1

**SIP Settings**

Active SIP Account

Number: ChangeMe

SIP Local Port: 5060 (1025-65535)

SIP Server Address: 127.0.0.1

SIP Server Port: 5060 (1-65535)

REGISTER Server Address: 127.0.0.1

REGISTER Server Port: 5060 (1-65535)

SIP Service Domain: 127.0.0.1

Send Caller ID

**Authentication**

User Name: ChangeMe

Password: .....

Apply Reset Advanced Setup

With the account information your ITSP provider provided now you may start.

**Step 1.** Open the web browser from your workstation to connect to the Prestige by entering the Management IP address of the Prestige (LAN IP address). The default management IP of Prestige is 192.168.1.1.

**Step 2.** Enter the administrator password appear on the page of login and click on login. The default is '1234'

**Step 3.** On the left column click on **VoIP** to bring you to VoIP configuration menu than click on **SIP**. While in the **SIP Settings** page use the account selector on upper right of the page to select the SIP account you will like to configure.

**Step 4.** Check active sip box if you like to use this account and fill in the account information the ITSP provided you in the **SIP setting** category. Which will normally include you **SIP number, SIP local port, SIP server address, SIP server port, Register server port, Register server address, SIP service domain.**

**Step 5.** In the **Authentication** category fill in the User Name and authentication password your ITSP provided to you.

**Step 6.** If you wish to send caller ID check the check box in the Caller ID category, if you do not wish to send out caller ID leave the check box uncheck.

**Step 7.** Click on **Apply** to save the setting and take effect. If you would like to configure the 2nd SIP account, please select SIP2 by using the SIP account selector than follow step 1 to 8 to complete the 2nd account setup.

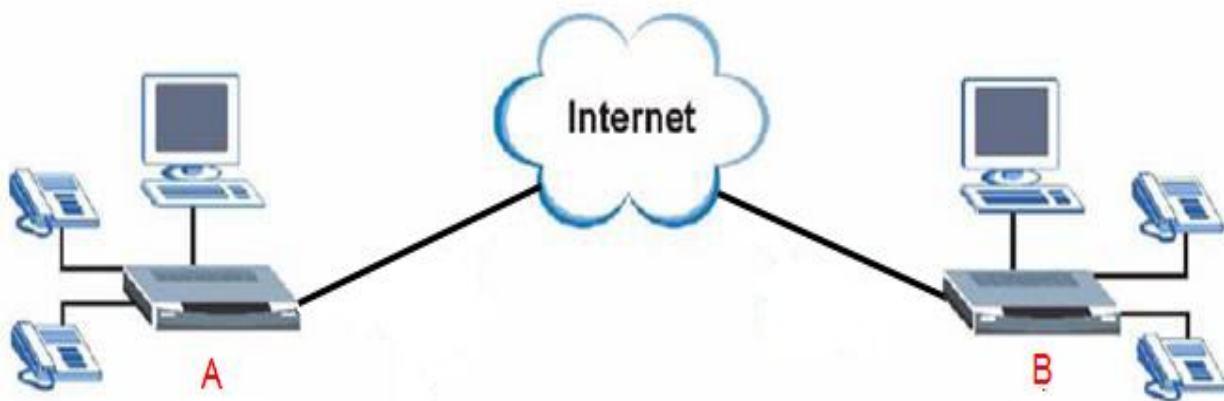
*Each field's detail description on this page is listed below.*

Label	Description
<b>SIP Account</b>	You can configure the Prestige to use multiple SIP accounts. Select one to configure its settings on the Prestige.
<b>SIP Number</b>	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.
<b>SIP Local Port</b>	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.
<b>SIP Server</b>	Type the IP address of the SIP server in this field.

<b>Address</b>	
<b>SIP Server Port</b>	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.
<b>REGISTER Server Address</b>	<p>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.</p> <p>Enter the SIP register server's address in this field.</p> <p><b>If you were not given a register server address, then enter the address from the SIP Server Address field again here.</b></p>
<b>REGISTER Server Port</b>	<p>Enter the SIP register server's listening port for SIP in this field.</p> <p><b>If you were not given a register server port, then enter the port from the SIP Server Port field again here.</b></p>
<b>SIP Service Domain</b>	<p>A SIP service domain is the domain name that comes after the @ symbol in a full SIP URI.</p> <p>Enter the SIP service domain name in this field. You can use up to 127 ASCII Extended set characters.</p>
<b>User Name</b>	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.
<b>Password</b>	Type the password associated with the user name above. Use ASCII Extended set characters.
<b>Send Caller ID</b>	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.
<b>Advanced Setup</b>	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.
<b>Apply</b>	Click <b>Apply</b> to save your changes back to the Prestige.
<b>Reset</b>	Click <b>Reset</b> to begin configuring this screen afresh.

## Peer to Peer call

### Topology



### Topology Explanation

1. Device A and B located at Internet.
2. Device A and B WAN interface is Public Static IP (220.130.46.197 and 220.130.46.198).
3. SIP number for device A and B is 197 and 198.

### Preparation and Steps

1. Install the device properly in user's networking topology.
2. Setup device's WAN connection.
3. Configuring SIP / VoIP related settings in device A and B.

There are two ways to make IP to IP call.

(1) Make you can call by speed dial like '#01' defined in the phone book.

You need to configure the self SIP number at VOIP screen and callee's IP address in the phone book

Note that there are 10 speed dial can be configured only so far.

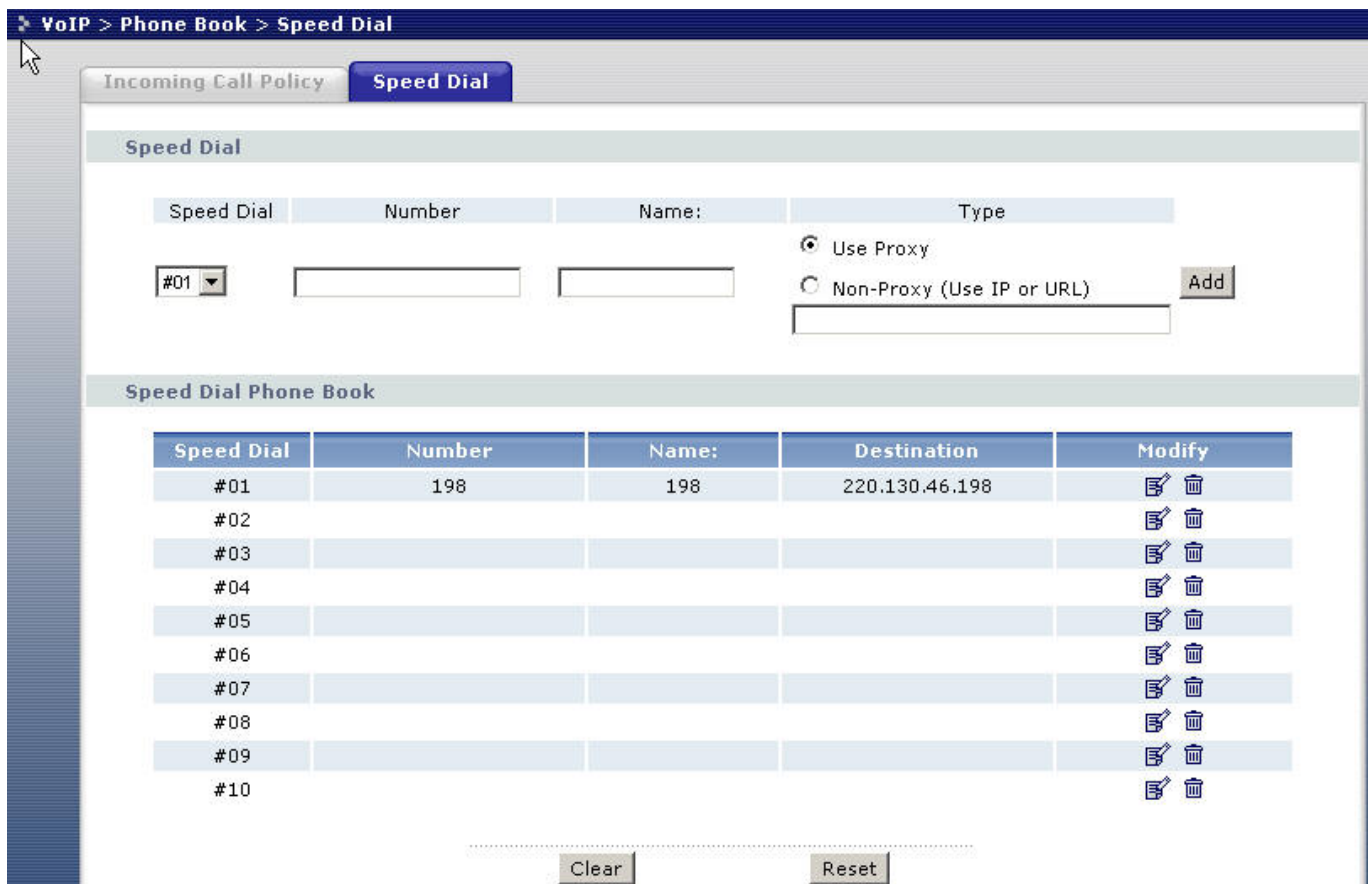
(2) Make you can call by callee's SIP number

You need to configure the self SIP number and put callee's IP address at SIP server, SIP proxy, Domain

server all in the VOIP screen.

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

The screenshot shows the 'SIP Settings' configuration page in a web browser. The breadcrumb navigation at the top reads 'VoIP > SIP > SIP Settings'. Below this, there are two tabs: 'SIP Settings' (selected) and 'QoS'. The 'SIP Account' is set to 'SIP1'. The 'SIP Settings' section includes a checked 'Active SIP Account' checkbox and several input fields: 'Number' (197), 'SIP Local Port' (5060, with '(1025-65535)' in parentheses), 'SIP Server Address' (220.130.46.198), 'SIP Server Port' (5060, with '(1-65535)' in parentheses), 'REGISTER Server Address' (220.130.46.198), 'REGISTER Server Port' (5060, with '(1-65535)' in parentheses), and 'SIP Service Domain' (220.130.46.198). There is also a checked 'Send Caller ID' checkbox. The 'Authentication' section contains 'User Name' (ChangeMe) and 'Password' (represented by 10 dots). At the bottom, there are three buttons: 'Apply', 'Reset', and 'Advanced Setup'.



1. Setup WEB GUI VoIP, enter device A's number in the SIP number column.
2. Fill in device B's IP into SIP server address, Register server address... as example.
3. Setup speed dial, put device B's information into the column.

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

VoIP > SIP > SIP Settings

SIP Settings    QoS

SIP Account : SIP1

**SIP Settings**

Active SIP Account

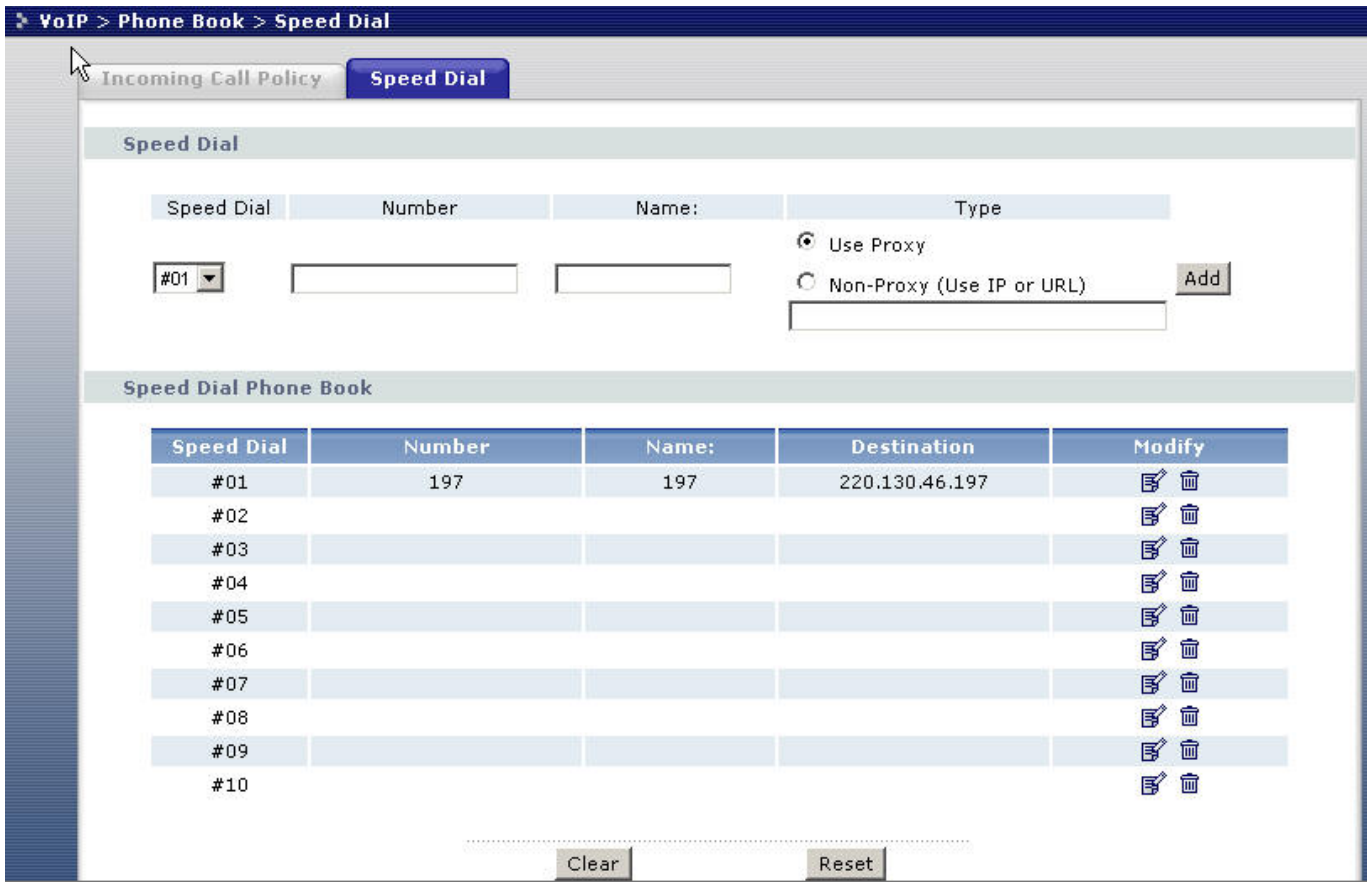
Number	198
SIP Local Port	5060 (1025-65535)
SIP Server Address	220.130.46.197
SIP Server Port	5060 (1-65535)
REGISTER Server Address	220.130.46.197
REGISTER Server Port	5060 (1-65535)
SIP Service Domain	220.130.46.197

Send Caller ID

**Authentication**

User Name	ChangeMe
Password	••••••••

Apply    Reset    Advanced Setup



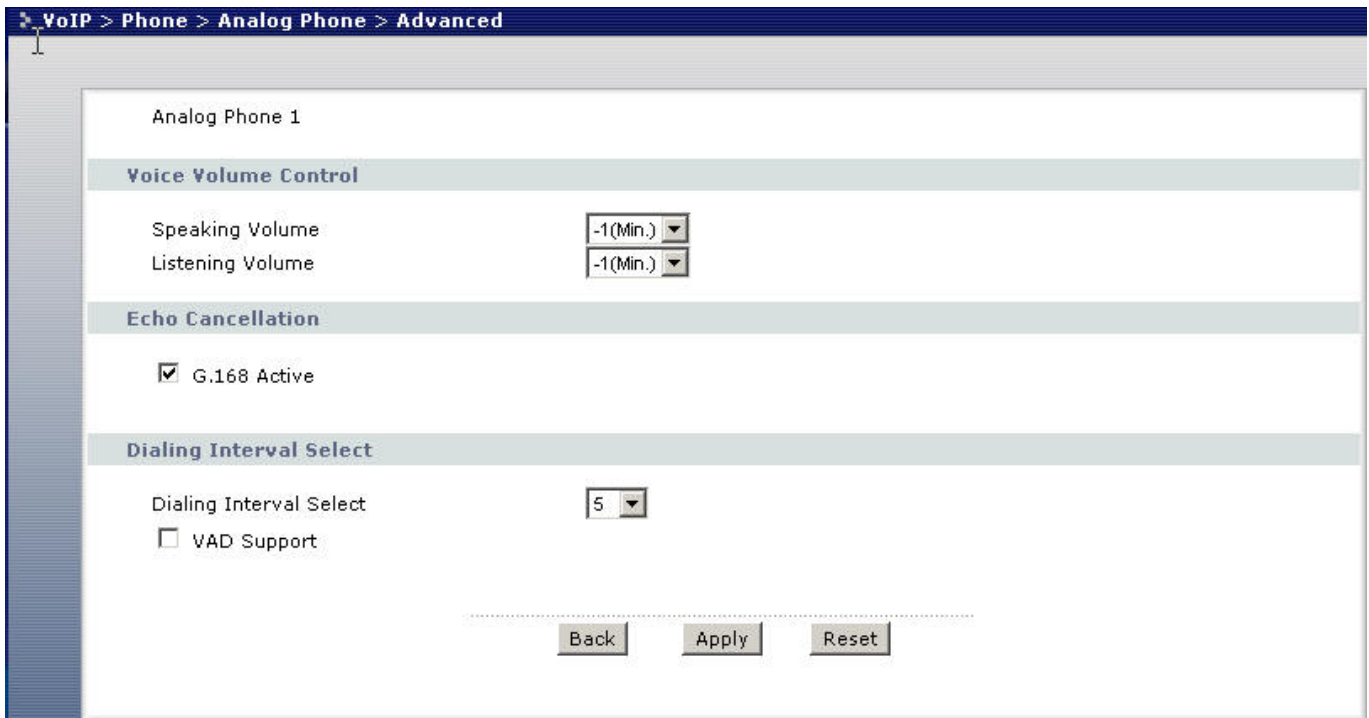
1. Setup WEB GUI VoIP, enter device B's number in the SIP number column.
2. Fill in device A's IP into SIP server address, Register server address... as example.
3. Setup speed dial, put device A's information into the column.

After completing the setting, you can dial #01 from the phone under device A, then the phone under device B will ring.

### Phone port settings

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





To configure the phone port setting please follow the below step.

**Step 1.** Open the web browser from your workstation to connect to the Prestige by entering the Management IP address of the Prestige. The default management IP of Prestige is 192.168.1.1.

**Step 2.** Enter the administrator password appear on the page of login and click on login. The default is '1234'

**Step 3.** On the left column click on **VoIP -> Phone -> Analog Phone -> Advanced Setup** to bring you to voice function menu.

**Step 4.** Change the phone port parameter as you desired and click **Apply** when you are finish to save and let the setting to take effect.

*Each field's detail description is listed below.*

Label	Description
<b>Speaking Volume</b>	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.
<b>Listening Volume</b>	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.
<b>G.168 Active</b>	Select this check box to cancel the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
<b>VAD Support</b>	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.
<b>Dialing Interval</b>	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.
<b>Apply</b>	Click <b>Apply</b> to save your changes back to the Prestige.
<b>Reset</b>	Click <b>Reset</b> to begin configuring this screen afresh.

---

### **Advanced voice settings configuration**

Click **VoIP** in the navigation panel and then **SIP** to open the **SIP Settings**. Select a SIP account and then click **Advanced Settings** to display the following screen. Advanced voice settings configuration allows user to modify SIP server related settings, RTP port range, preferred compression type (codec), DTMF type and Message Waiting Indication (MWI)

SIP Account : SIP1

---

**SIP Server Settings**

URL Type: SIP

Expiration Duration: 3600 (20-65535) sec

Register Re-send timer: 180 (1-65535) sec

Session Expires: 180 (30-3600) sec

Min-SE: 30 (20-1800) sec

---

**RTP Port Range**

Start Port: 50000 (1025-65535)

End Port: 65535 (1025-65535)

---

**Voice Compression**

Primary Compression Type: G.711A

Secondary Compression Type: G.729

Third Compression Type: G.729

DTMF Mode: RFC 2833

---

**MWI (Message Waiting Indication)**

Enable

Expiration Time: 1800 (1-65535) sec

---

**Fax Option**

G.711 Fax Passthrough       T.38 Fax Relay

---

**Call Forward**

Call Forward Table: Table 1

.....

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

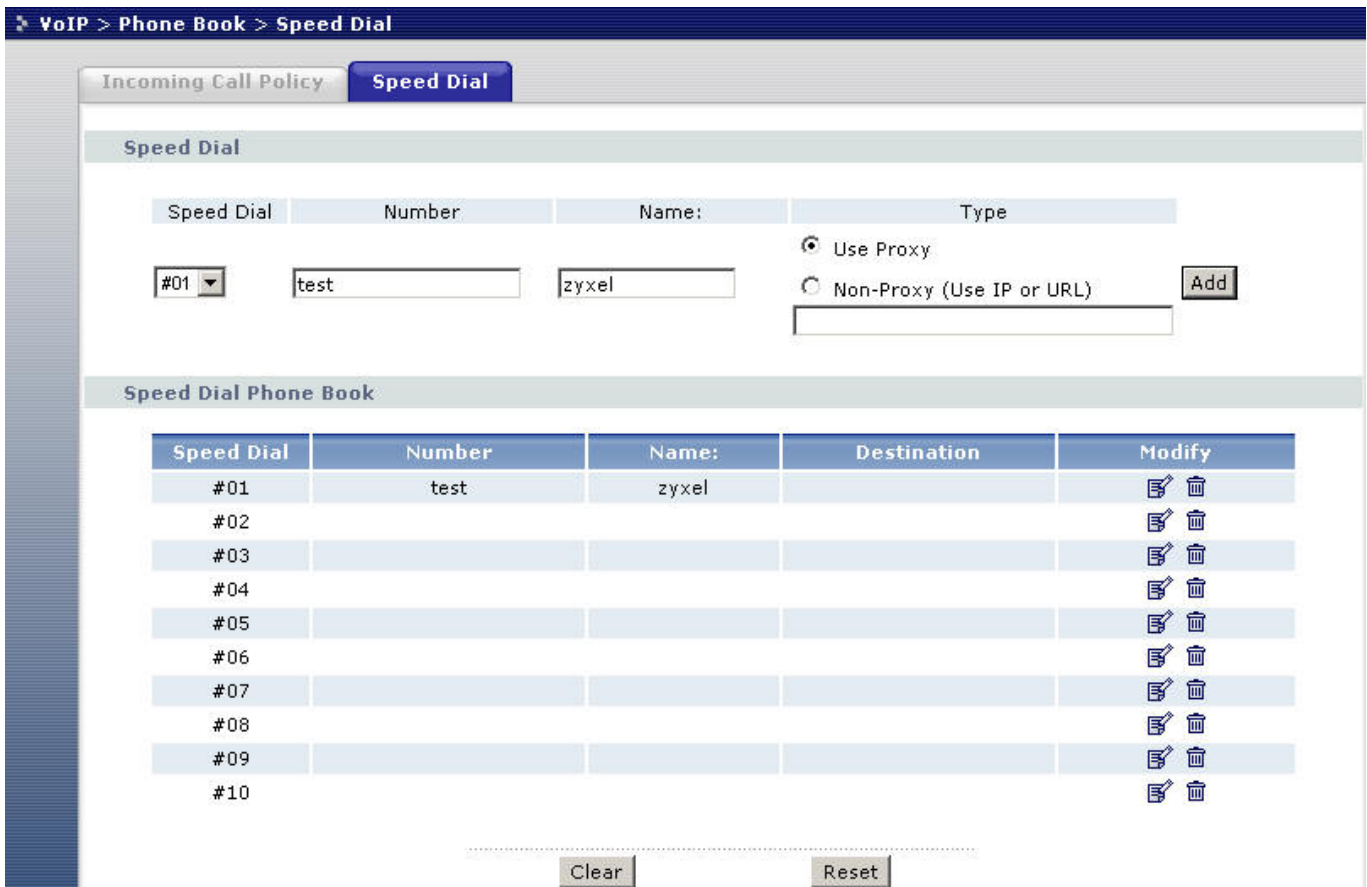
Label	Description
<b>SIP Account</b>	This read-only field displays the number of the SIP account that you are configuring. The changes that you save in this page affect the Prestige's settings with the SIP account displayed here..

<b>URL Type</b>	<p>Select <b>SIP</b> to have the Prestige include the domain name with the SIP number in the SIP messages that it sends.</p> <p>Select <b>TEL</b> to have the Prestige use the SIP number without a domain name in the SIP messages that it sends.</p>
<b>Expiration Duration</b>	<p>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.</p>
<b>Register Re-send Timer</b>	<p>Use this field to set how long the Prestige waits before sending a repeat registration request if a registration attempt fails or there is no response from the registration server.</p>
<b>Session Expires</b>	<p>Use this field to set the longest time that the Prestige will allow a SIP session to remain idle (without traffic) before dropping it</p>
<b>Min-SE</b>	<p>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.?</p> <p>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.</p>
<b>RTP Port Range</b>	<p>Real time Transport Protocol 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.</p>
<b>DTMF Mode</b>	<p>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.</p>

	<p>Select <b>RFC 2833</b> to send the DTMF tones in RTP packets.</p> <p>Select <b>PCM</b> (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.</p> <p>Select <b>SIP INFO</b> to send the DTMF tones in SIP messages.</p>
<b>MWI (Message Waiting Indication)</b>	<p>Enable Message Waiting Indication (MWI) to have your phone give you a message–waiting (beeping) dial tone when you have a voice message(s). Your voice service provider must have a messaging system that supports this feature.</p>
<b>Expiration Time</b>	<p>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.</p>
<b>Call Forward Table</b>	<p>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.</p>
<b>Back</b>	<p>Click <b>Back</b> to return to the previous screen without saving configuration changes.</p>
<b>Apply</b>	<p>Click <b>Apply</b> to save your changes back to the Prestige.</p>

**Phone book Speed dial**

Prestige allows you to configure up to 10 SIP numbers in the phone book for speed dial.



To configure phone book for speed dial please follow the below step.

**Step 1.** Open the web browser from your workstation to connect to the Prestige by entering the Management IP address of the Prestige. The default management IP of Prestige is 192.168.1.1.

**Step 2.** Enter the administrator password appear on the page of login and click on login. The default is '1234'

**Step 3.** On the left column click on **VoIP -> Phone Book -> Speed Dial** to bring you to **Speed Dial** page to enter speed dial configuration page.

**Step 4.** Select the entry number you wish to add to the phone book by the entry selector located under add new entry category on the speed dial field.

**Step 5.** Fill in the SIP number of the remote party and a descriptive name and click on the radio button to select either to use proxy or entering static IP or URL remote peer.

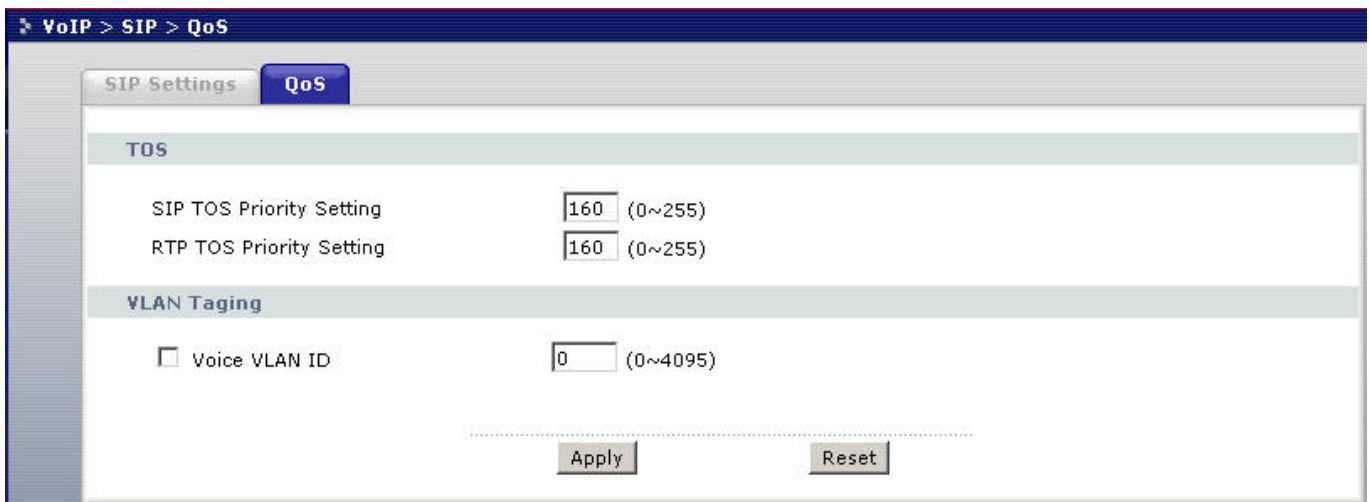
Step 6. Click on Add button when you are finish to add the entry to the phone book.

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

Label	Description
<b>Speed Dial</b>	Select a speed dial key combination from the drop-down list box.
<b>SIP Number</b>	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.
<b>Name</b>	Enter a descriptive name to identify the party that you will use this entry to call. You can use up to 127 ASCII characters.
<b>Type</b>	Select <b>Use Proxy</b> if calls to this party use your SIP account configured in the VoIP screen.  Select <b>Non-Proxy (Use IP or URL)</b> 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).
<b>Add</b>	Click this button to save the entry in the speed dial phone book. The speed dial entry displays in the <b>Speed Dial Phone Book</b> section of the screen.
<b>Speed Dial Phone Book</b>	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.
<b>Speed Dial</b>	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.
<b>Name</b>	This is the descriptive name of the party that you will use this speed dial entry to call.
<b>SIP Number</b>	This is the SIP number of the party that you will call.
<b>Type</b>	This field displays <b>Use Proxy</b> 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.
<b>Delete</b>	Click this button to remove an entry from the speed dial phonebook.
<b>Edit</b>	Click this button to change the speed dial entry. The speed dial entry displays in the <b>Add New Entry</b> section of the screen where you can edit it.
<b>Clear</b>	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.



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

Label	Description
<b>SIP TOS Priority</b>	Type a priority for voice transmissions. The Prestige applies Type of Service priority tags with this priority to voice traffic that it transmits.
<b>RTP TOS Priority</b>	Type a priority for voice transmissions. The Prestige applies Type of Service priority tags with this priority to RTP traffic that it transmits.
<b>Voice VLAN ID</b>	<p>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.</p> <p>Type the VLAN ID (VID) from 1 to 4095 for the Prestige to add to voice Ethernet frames that it sends out to the network.</p> <p>Disable VLAN tagging if the Prestige does not need to be a member of a</p>



	VLAN group to communicate with the SIP server.
<b>Apply</b>	Click <b>Apply</b> to save your changes back to the Prestige.

**Call Forwarding setup**

Call forwarding function allows users to determine handling of incoming calls. For example, a user may wish to decide that all incoming calls will ring his cell phone as well. The following screenshot shows how users can use this screen to configure the Prestige to block or redirect calls. You can configure a different call forwarding table for each SIP account or use the same call forwarding table for both.

VoIP > Phone Book > Incoming Call Policy

Table Number: Table 1

**Forward to Number Setup**

Unconditional Forward to Number

Busy Forward to Number

No Answer Forward to Number

No Answer Waiting Time  (Second)

**Advanced Setup**

#	Activate	Incoming Call Number	Forward to Number	Condition
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional

**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.

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

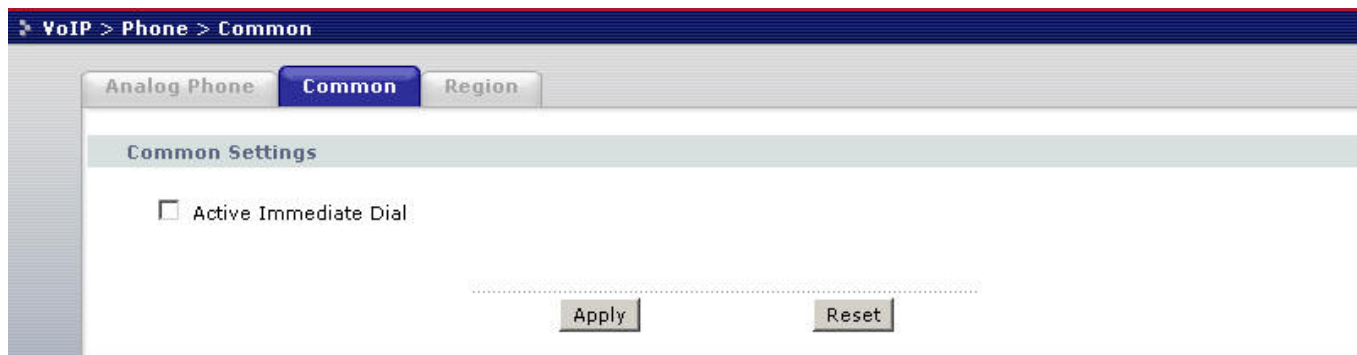
<b>Label</b>	<b>Description</b>
<b>Table Number</b>	Select which call forwarding table you want to configure. You can configure a different call forwarding table for each SIP account or use the same call forwarding table for both.
	The following applies to the number fields in this screen.  For a SIP number, use the number or text that comes before the @ symbol in a full SIP URI.
<b>Forward to Number Setup</b>	These are the global call forwarding settings that define the default action to take on incoming calls that do not match any of the <b>Advanced Setup</b> call forwarding entries.
<b>Unconditional Forward to Number</b>	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.
<b>Busy Forward to Number</b>	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.
<b>No Answer</b>	Enable this feature to have the Prestige forward incoming calls to the

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

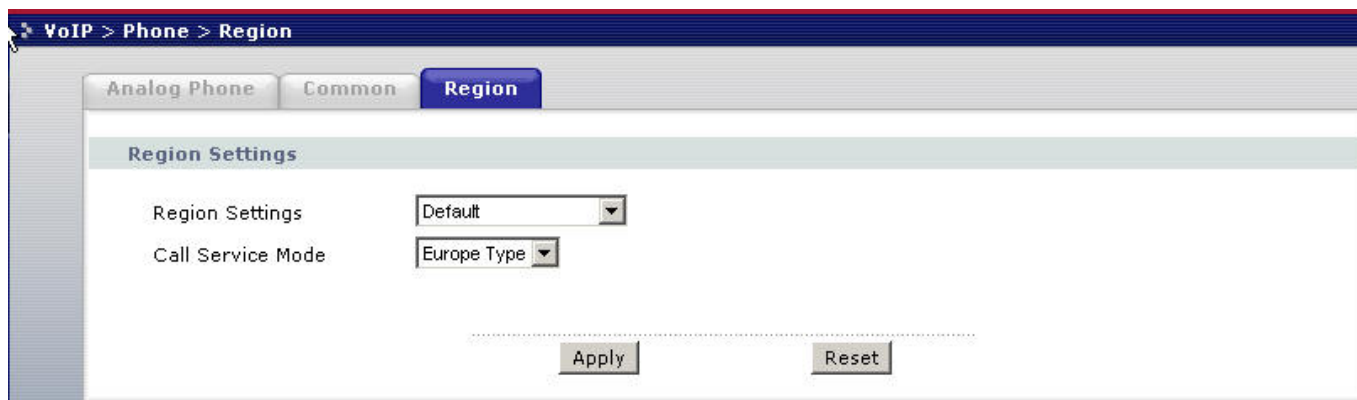
	the <b>Incoming Call Number</b> field.
--	--

**Voice – Common Settings**

Click **VoIP -> Phone -> Common** to display the following screen. Use this screen to configure Immediate Dial



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



Label	Description
-------	-------------

<b>Region Settings</b>	Use the drop-down list box to select the country where your Prestige is located.
<b>Immediate Dial</b>	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).
<b>Call Service Mode</b>	<p>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.</p> <p>Select <b>Europe Type</b> to use the supplementary phone services in European mode.</p> <p>Select <b>USA Type</b> to use the supplementary phone services American mode.</p> <p>See your User's Guide for supplementary phone service details.</p> <p><b>To take full advantage of the supplementary phone services available though the Prestige's phone ports, you may need to subscribe to the services from your voice service provider.</b></p>
<b>Back</b>	Click <b>Back</b> to return to the previous screen.
<b>Apply</b>	Click <b>Apply</b> to save your changes back to the Prestige.

## 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 Web download site as they become available.

### **How do I access the embedded web configurator?**

The Web configurator a user friendly configuration interface via user's web browser, which can be access by typing in the LAN IP address of the Prestige in users web browser. To access the Prestige's web configurator via web browser, the configuration PC must be in the same IP segment of Prestige and Prestige must be reachable to the configuration station. (By default the Prestige LAN IP is 192.168.1.1)

### **What is the default LAN IP address and Password? Moreover, 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 menu under "LAN"->LAN TCP/IP, the default password is 1234. You can change the password once you enter the web configuration menu under "SYSTEM" and press the Password tab. At the password screen type in the old password and the new password and retype to confirm than press "Apply" button to save the change.

### **How do I upload the ZyNOS firmware code via embeded web configurator?**

The procedure for uploading ZyNOS via embeded web configurator is as follows.

- a. Log on into the web configurator.
- b. Press "MAINTENANCE" from the left menu.
- c. Press "F/W Upload" tab.
- d. Press "browse" button and point to the directory where the firmware you want to upload is kept and press "Upload" button.
- e. It will prompt you the firmware is upload successful and Prestige will reboot.

### **How do I upgrade/backup the ZyNOS firmware by using FTP client program via LAN?**

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

- a. To upgrade firmware, use FTP client program to put firmware in file 'ras' in the Prestige. After data transfer is finished, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself. Note: Do not power off the unit after upload the file via ftp until the system LED have become steady light up. Fail to due so may result in update fail and require RMA.
- b. To backup your firmware, use the FTP client program to get file 'ras' from the Prestige.

### **How do I upload or backup ROMFILE via web configurator?**

In some situations, you may need to upload the ROMFILE, restore to previous saved configuration, or the need of resetting SMT to factory default.

The procedure for uploading ROMFILE via the web configurator is as follows.

- a. Log on into the web configurator.
- b. Press "MAINTENANCE" from the left menu.
- c. Press "Configuration" tab.
- d. Press "Restore" tab and press browse button point to the directory where the romfile you want to upload is stored.
- e. Press "Upload" button.

The procedure for backup ROMFILE via the web configurator is as follow

- a. Log on into the web configurator.
- b. Press "MAINTENANCE" from the left menu.
- c. Press "Configuration" tab.
- d. Press "Backup" button, a pop up windows will ask you where to store the back up romfile.
- e. Press "Save file" and browse to where you want the file be save.
- f. Press "Save" button.

### **How do I backup/restore configurations by using FTP client program via LAN?**

- a. Use the a FTP client program in your PC (such as cuteftp, wsftp client) to login to your Prestige.
- b. To backup the configurations, use FTP client program to get file 'rom-0' from the Prestige.

- c. To restore the configurations, use the FTP client program to put your configuration in file ROM-0 in the Prestige.

### **Why can't I make Telnet to Prestige from WAN?**

There are three possible reasons that Telnet from WAN is blocked.

- a. You have not enable Telnet service on WAN interface in Menu 24.11.
- b. Telnet service is enabled but your host IP is not the secured host entered in Menu 24.11. In this case, the error message 'Client IP is not allowed!' will appear on the Telnet screen.
- c. The default filter rule 3 (Telnet\_FTP\_WAN) is applied in the Input Protocol field in menu 11.5.

### **What should I do if I forget the system password?**

In case you forget the system password. You can reset the unit back to factory default. You can reset the unit by using a sharp pointed object such as a pen and press and hold down the “reset” button for 5 second or until the power LED starts to blink than release. The unit is than reset back to factory default. The reset button is located near by the power jack on the unit back panel.

*Note: By reset the unit back to factory default you will lost all your previous settings.*

### **What is SUA? When should I use SUA?**

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

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



**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 implementation and trade name for functioning PAT which is a specific type of NAT. SUA (or PAT for NAT) translates address into port mapping.

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

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

**How many network users can the SUA/NAT support?**

The Prestige does not limit the number of the users but the number of the sessions. The Prestige supports 1024 sessions that you can use the 'ip nat iface enif0 disp' command in menu 24.8 to view the current active sessions.

**What are Device filters and Protocol filters?**

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

**Why can't I configure device filters or protocol filters?**

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

---

## Product FAQ

### **What is the Prestige Integrated Access Device?**

The Prestige series fulfills a range of application environments, from small and medium businesses, SOHO, or Telecommuters, to home user or education applications. Prestige's design helps users to save expenses, minimize maintenance, and simultaneously provide a high quality networking environment.

The Prestige series is a robust solution complete with everything needed for providing Internet access to multiple workstations through ADSL. The IAD is equipped with 1 auto-MDI/MDIX 10/100Mbps Ethernet LAN port, 1 ADSL WAN port. It is the most simple and affordable solution for multiple and instant broadband Internet access router.

Virtually all-popular applications over Internet, such as Web, E-Mail, FTP, Telnet, Gopher, are supported. Prestige is designed for SOHO, branch offices, workgroups, and educational users.

### **Will the Prestige work with my Internet connection?**

The Prestige is designed to be compatible major ISP utilize ADSL as a broadband service. Prestige IAD offers an Ethernet port to connect to your computer so the Prestige is placed in the line between the computer and your ISP. If your ISP supports PPPoE/PPPoA you can also use the Prestige, because PPPoE/PPPoA had been supported in the Prestige.

### **What do I need to use the Prestige?**

You need an ADSL modem/router to use with ADSL line, Prestige is an idea device for such application. The Prestige has one Ethernet ports: LAN port and one ADSL WAN port. You should connect the computer to the LAN port and connect the ADSL line to the WAN port. If the ISP uses PPPoE or PPPoA you need the user account to enter in the Prestige.

### **What is PPPoE?**

PPPoE stands for **P**oint-to-**P**oint **P**rotocol over **E**thernet that is an IETF draft standard specifying how a computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to the high-speed data networks via a familiar PPP dialer such as 'Dial-Up Networking' user interface. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management. There are some service providers running of PPPoE today. Before configuring PPPoE in the Prestige, please 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 provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the Prestige if the ISP uses PPPoE.

**Why does my provider use PPPoE?**

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

**Which Internet Applications can I use with the Prestige?**

Most common applications include MIRC, PPTP, ICQ, Cu-SeeMe, NetMeeting, IP/TV, RealPlayer, VDOLive, Quake, QuakeII, QuakeIII, StarCraft, & Quick Time.

**How can I configure the Prestige?**

- a. Telnet remote management- Menu driven user interface for easy remote management
- b. Web browser- web server embedded for easy configurations

**What network interface does the Prestige support?**

The Prestige supports 10/100M Ethernet to connect to the LAN computer or hub/switch and 10/100M ADSL interface to the ISP.

**What can we do with Prestige?**

Browse the World Wide Web (WWW), send and receive individual e-mail, and download software. These are just a few of many benefits you can enjoy when you put the whole office on-line with the Prestige Internet Access Sharing Router.

**Does Prestige support dynamic IP addressing?**

The Prestige supports either a static or dynamic IP address from ISP.

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

Internal IPs is sometimes referred to as virtual IPs. They are a group of up to 255 IPs that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP from ISP, instead, can be recognized or pinged by another real IP. The Prestige Internet Access Sharing Router works like an intelligent router that route between the virtual IP and the real IP.

**How does e-mail work through the Prestige?**

It depends on what kind of IP 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 Prestige Internet Access Device using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access right.

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 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 individual private and secured e-mail, if they have been assigned the proper access right.

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

Yes, it is possible because Prestige delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured in 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 the Internet IP address from ISP automatically if your ISP use DHCP as a method to assign IP address. The Prestige's internal DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

**How do I used the reset button, more over what field of parameter will be reset by reset button?**

You can used a sharp pointed object insert it into the little reset hole beside the power connector. Press down the reset button and hold down for approx 5 second, the unit will be reset. When the reset button is pressed the devices all parameter will be reset back to factory default include, password, and IP address.

The default IP address is 192.168.1.1, Password 1234.

**What network interface does the new Prestige series support?**

The new Prestige series support auto MDX/MDIX 10/100M Ethernet LAN port to connect to the computer or Switch on LAN and ADSL port on WAN.

---

**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.

**Can the Prestige support TFTP over WAN?**

Although TFTP should work over WAN as well, it is not recommended because of the potential data corruption problems.

**How fast can the data go?**

The speed of the ADSL is only one part of the equation. There are a combination of factors starting with how fast your PC can handle IP traffic, then how fast your PC to cable modem interface is, then how fast the cable modem system runs and how much congestion there is on the cable network, then how big a pipe there is at the head end to the rest of the Internet.

Different models of PCs and Macs are able to handle IP traffic at varying speeds. Very few can handle it at 30 Mbps.

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

Cable modems on the same node share bandwidth, which means that congestion is created when too many people are on simultaneously. One user downloading large graphic or video files can use a significant portion of shared bandwidth, slowing down access for other users in the same neighborhood.

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

To create the appearance of faster network access, service companies plan to store or "cache" frequently requested web sites and Usenet newsgroups on a server at their head-end. Storing data locally will remove some of the bottleneck at the backbone connection.

How fast can they go? In a perfect world (or lab) 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 Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the 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 only one subset of the NAT. The Prestige with ZyNOS V3.00 supports the most of the features of the NAT based on RFC 1631, and we call this feature as '**Multi-NAT**'. For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

### **When do I need Multi-NAT?**

- a. **Make local server accessible from outside Internet**

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

a. **Support Non-NAT Friendly Applications**

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

**What IP/Port mapping does Multi-NAT support?**

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

**1. One to One**

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

**2. Many to One**

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

**3. Many to Many Overload**

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

**4. Many to Many No Overload**

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

**5. Server**

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

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many-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 a NAT set with 2 rules, Many-to-One and Server. The Prestige now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple servers of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions that supported SUA 'visible' servers had to be of different types. The Prestige supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The Prestige supports 2 sets since there is only one remote node. The default SUA (Read Only) Set in menu 15.1 is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions.

**What is BOOTP/DHCP?**

BOOTP stands for Bootstrap Protocol. DHCP stands for Dynamic Host Configuration Protocol. Both are mechanisms to dynamically assign an IP address for a TCP/IP client by the server. In this case, the Prestige Internet Access Sharing Router is a BOOTP/DHCP server. Win95 and WinNT 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.



## **What is DDNS?**

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

Without DDNS, we always tell the users to use the WAN IP of the 312 to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the Prestige, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the 312.

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

## **When do I need DDNS service?**

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

## **What DDNS servers does the Prestige support?**

The DDNS servers the Prestige supports currently is [WWW.DYNDNS.ORG](http://WWW.DYNDNS.ORG) where you apply the DNS from and update the WAN IP to.

## **What is DDNS wildcard?**

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

## **Does the Prestige support DDNS wildcard?**

Yes, the Prestige supports DDNS wildcard that [WWW.DynDNS.ORG](http://WWW.DynDNS.ORG) supports. When using wildcard, you simply enter yourhost.dyndns.org in the **Host** field in Menu 1.1.

**Can the Prestige SUA handle IPsec packets sent by the VPN gateway behind Prestige?**

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

**How do I setup my Prestige for routing IPsec packets over SUA?**

For outgoing IPsec tunnels, no extra setting is required. For forwarding the inbound IPsec ESP tunnel, A 'Default' server set in menu 15 is required. It is because SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP of this server in Menu 15. Thus SUA is able to forward the incoming packets to the requested service behind SUA and the outside users access the server using the Prestige's WAN IP address. So, we have to configure the internal IPsec as a default server (unspecified service port) in menu 15 when it acts a server gateway.

**PSTN Lifeline FAQ****What is P2602 and what is the difference between P2602HW and P2602HWL?**

P2602HW is a SIP based VoIP analog telephone adapter. It allows you to send voice signals over the Internet or VoIP of IP via SIP protocol which is an internationally recognized standard for VoIP Technology.

The main difference between P2602HW and P2602HWL is in Lifeline support. P2602HWL supports PSTN lifeline function. A PSTN lifeline allows you to have VoIP phone service and PSTN phone service at the same time.

**What does Lifeline mean?**

Lifeline means the ability to reach specified emergency rescue authority (Police, Fire department etc.) as you can do on regular phone line in case emergency even if P2602HWL loses power.

**Do I need Lifeline?**

Not everyone needs lifeline support on VoIP telephone adapter. It depends on the government authority or ITSP provider. As in some countries lifeline support are mandatory by law.

**Can I connect more than one phone on the phone port?**

Yes, P2602HWL - 6xC supports REN (Ringer Equivalence Number), it can determine the number of devices that is connected to the phone line. P2602HWL - 6xC can support up to three devices per telephone port.

**Can I receive incoming PSTN call through P2602HWL- 6xC?**

Yes, P2602HWL has a line port for connecting a PSTN line. Thus enable you to receive incoming PSTN calls.

**Can I make an outgoing PSTN call through P2602HWL – 6xC?**

Yes, P2602HWL - 6xC allows you to make outgoing PSTN call via a prefix number that is defined in the configurable lifeline table. It allows you to store up to 9 pre-stored numbers. If P2602HWL- 6xC lost power it will by pass to PSTN line to allow you to call out as you where on regular PSTN phone.

**VoIP FAQ****What is Voice over IP?**

Voice over IP is an emerging technology based on open standards of IEEE, fundamentally the Internet Protocol, that allows voice data to travel across the Internet. There are many method to used this technology, the most common and well known are SIP, and H.323.

**How does Voice over IP work?**

Basically VoIP is a technic to send voice information in digital form in discrete packets over digital network rather than by using traditional circuit switch (PSTN). To do so we will need an analog to digital converter on sender side to translate the voice (analog signal) to digital than transmit it, and on the receiver end it will also need an analog to digital converter to covert the digital signal back to analog to the person being called can heard the voice.

**Why use VoIP?**

Traditionally telephony carrier use circuit switching for carrying voice traffic. As circuit switching is designed to carry voice and it does it very well. Than why use IP for voice? As broadband booms, and technology evolve. People now want to communicate through various way not just voice such as email, instant messaging, video and so on. Traditional telephony can not evolve as quickly as the demand and develop new feature on circuit switch takes much time and money. IP is an already exist standard and many type of service

already runs on IP, by using IP as a platform integrate service is now possible and low cost where traditional circuit may take long time to achieve.

### **What is the relationship between codec and VoIP?**

In order to transfer voice (analog signal) over IP it first need to be digitized. Codec is a technic to digitize analog signal to digital and vice versa. There are various speech codec available and can be used with VoIP each with it's advantage and disadvantage.

### **What advantage does Voice over IP can provide?**

The advantage of VoIP is it can provide advance services such as joining e-mail, instant messaging, video, voice mail all together. Where current circuit switching (PSTN) can not.

### **What is the difference between H.323 and SIP?**

H.323 and SIP are proposed by different group 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, perspective of view. Where as 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 an person can hear the voice on the opposite end.

### **How are voice quality normally rated?**

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

**What is codec?**

Codec is a algorithm which converts analog signal into digital signal and vice versa. There are three main type of waveform codec, source codec, and hybrid codec. Each consume different amount of bandwidth and provide different voice quality level.

**What is the relation of codec and VoIP?**

As VoIP is a general term send voice information in digital form in discrete packets over digital network and this digital network is public network, thus there maybe other packet such data packet uses network at the same time. The codec choose is related to how much bandwidth voice packet will consume. In bandwidthwise aspect the smaller amount of bandwidth used the better. But in voice aspect the higher quality the better.

**What codec does Prestige support?**

Prestige supports the following commonly used codec.

- 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 ZyXEL device is shipped preconfigured to use u-law or a-law according to specific country. If for special reason this setting needed to be changed. It can be modify through device CI command through telnet. For the command please refer to the CI command list in the firmware release note.

**Which codec should I choose?**

As which codec choose is depending on what codec is supported on both end of the VoIP host. Generally a codec with low bandwidth consumption and high voice quality is a good codec .

**What do I need in order to use SIP?**

The minimum required to use VoIP is as follow.

1. A high-speed Internet connection. This can be a cable modem, or a high-speed network services such as ISDN, DSL or a T-1 link. The need of the bandwidth required will depend on the amount of telephone traffic will be in your network.

2. A PC with VoIP software installed or a hardware VoIP box such as ATA or device like Prestige 2602 VoIP station router.
3. An account with a VoIP provider such as an ITSP. The account can be configured to recognize your calls automatically, or you can require the users to enter their unique account numbers issued.

### **Unable to register with the SIP server?**

If you are unable to register with SIP server.

1. Make sure the Internet is reachable and the SIP register server is reachable. If your register server uses domain name make sure DNS name can be resolved. If you are using static WAN IP make sure DNS server is configured correctly on your Prestige.
2. Make sure the SIP account is correct and the password is key in correctly.
3. Check if there is NAT router before it. Prestige is a VoIP station gateway. We do not suggest to have an NAT router before it as it may cause many unexpected problem. If you have an NAT router before it we suggest to use a VoIP ATA (VoIP Analog Telephone Adapter) such as Prestige ATA series.

### **I can register but can not establish a call?**

If you can register to server but can not make a call very likely there is NAT router or firewall before it which is blocking it. We do not suggest to have an NAT router before it as it may cause many unexpected problem. If you have an NAT router before it we suggest to use a VoIP ATA (VoIP Analog Telephone Adapter) such as Prestige ATA series.

If the problem is a firewall before it. Please check with the firewall manager, make sure the SIP protocol is allow to pass-through firewall, and the range of RTP port is allowed through firewall.

### **I can make a call but the voice only goes one way not bothway?**

If you can register to server and I can make a call signal establishment but the voice only goes one way. In this case it is very likely there are NAT router or firewall before it, please see NAT/firewall related question above.

### **I can receive a call but the voice only goes one way not bothway?**

If you can register to server but can only make out going call but can not receive incoming calls or the incoming call signal establishment can be made but voice only goes one way very likely there is NAT/firewall router before it, please see NAT/firewall related question above for tips to troubleshoot.

**If all the about have been tried, but register still fail what should I do?**

In such case, please contact your local vendor for support. If they can't help out the problem they will escalate your problem to ZyXEL tech center. To report a problem please prepared below info.

1. Serial number of the device.
2. SIP Call server type and vendor.
3. Your device firmware version and romfile with password.
4. Detail information what you have tried to resolve the problem.

**I suspect there is a hardware problem with my Prestige what should I do?**

Please follow the troubleshooting section in the user's guide for brief hardware troubleshooting and diagnostic tips. If you are sure there is a hardware problem after following the hardware diagnostic tips in the user's guide. Please contact your ZyXEL local vendor to send the device in for RMA service.

---

**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 untrusted network. The firewall can be thought of two mechanisms. One to block the traffic, and the other to permit traffic.

**What makes 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 to determine if an inbound connection is allowed through the firewall to the private LAN. The Prestige supports Network Address Translation (NAT), which translates the private local addresses to one or multiple public addresses. This adds a level of security since the clients on the private LAN are invisible to the Internet.

## **What are the basic types of firewalls?**

Conceptually, there are three types of firewalls:

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

Packet Filtering Firewalls generally make their decisions based on the header information in individual packets. These header information include the source, destination addresses and ports of the packets.

Application-level Firewalls generally are hosts running proxy servers, which permit no traffic directly between networks, and which 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 this device 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 kind of firewall is the Prestige?**

1. The Prestige's firewall inspects packets contents and IP headers. It is applicable to all protocols, that understands data in the packet is intended for other layers, from network layer up to the application layer.
2. The Prestige's firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and 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 enhance the filtering process and control the network session rather than control 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 packet filtering and NAT built-in?**

With the spectacular growth of the Internet and online access, companies that do business on the Internet face greater security threats. Although packet filter and NAT restrict access to particular computers and networks, however, for the other companies this security may be insufficient, because packets filters typically cannot maintain session state. Thus, for greater security, a firewall is considered.

## **What is Denials 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 Ping of Death attack?**

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

## **What is Teardrop attack?**

Teardrop attack exploits weakness in the reassemble of the 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 SYN Flood attack?**

SYN attack floods 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 the

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 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 Brute-force attack?**

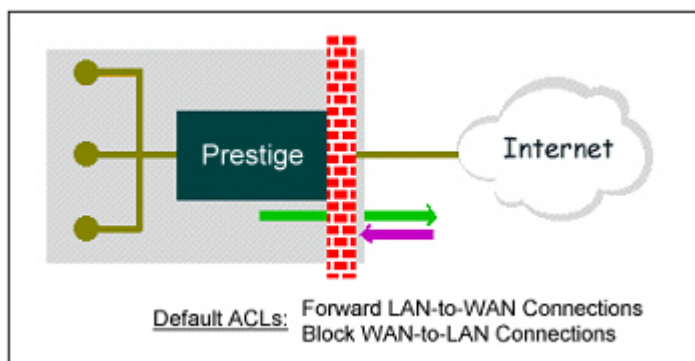
A Brute-force attack, such as 'Smurf' attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address of each packet is the broadcast address of the network, the router will 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 packet, 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 flood of broadcast traffic consumes all available bandwidth, making communications impossible.

### **What is IP Spoofing attack?**

Many DoS attacks also use IP Spoofing as part of their attack. 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 in Prestige?**

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



### How can I protect against IP spoofing attacks?

The Prestige's firewall will automatically detect the IP spoofing and drop it if the firewall is turned on. If the firewall is not turned on we can configure a filter set to block the IP spoofing attacks. The basic scheme is as follows:

For the input data filter:

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

Filter rule setup:

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

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

For the output data filters:

- Deny bounceback packet
- Allow packets that originate from us

Filter rule setup:

- Filter Type =TCP/IP Filter Rule

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

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

---

## Content Filter FAQ

### **What types of content filter does Prestige provide?**

### **Can I have different policies in effect for different times of the day or week?**

Yes, but only one blocking period of time is supported currently on ZyXEL appliance.

### **Can I override (block or allow) certain URLs by wording?**

Yes, you can use key word blocking to achieve this.

### **How many URL keywords does Prestige support?**

**64 keywords are supported.**

---

## IPSec FAQ

### **What is VPN?**

A VPN gives users a secure link to access corporate network 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 VPN?**

There are some reasons to use a VPN. The most common reasons are because of security and cost.

### **Security**

#### 1). Authentication

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

#### 2). Encryption

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

### **Cost**

#### 1). Cut long distance phone charges

Because users typically dial the their local ISP for VPN, thus, long distance phone charge is reduced than making a long direct connection to the remote office.

#### 2).Reducing number of access lines

Many companies pay monthly charges for two types access lines: (1) high-speed links for their Internet access and (2) frame relay, ISDN Primary Rate Interface or T1 lines to carry data. A VPN may allow a company to carry the data traffic over its Internet access lines, thus reducing the need for some installed lines.

## **What are most common VPN protocols?**

There are currently three major tunneling protocols for VPNs. They 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. The

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

### **What is L2TP?**

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an 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 can protect any protocol that runs on top of IP, for instance TCP, UDP, and ICMP. The IPSec provides cryptographic security services. These services allow for 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 do encryption between computers. Since you have so many options, IPSec is truly the most extensible and complete network security solution.

### **What secure protocols does IPSec support?**

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

### **What are the differences between '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 security gateway to provide IPSec service for other machines lacking of IPSec capability.

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

There is no restriction that the IPSec hosts and the security gateway must be separate machines. Both IPSec protocols, AH and ESP, can operate in either transport mode and 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 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. Afterward, two VPN gateways use this negotiated keys and SPIs to send packets between 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 Phase 1 ID for?**

In IKE phase 1 negotiation, IP address of remote peer is treated as an indicator to decide which VPN rule must be used to serve the incoming request. However, in some application, remote VPN box or client software is using an IP address dynamically assigned from ISP, so Prestige needs additional information to make the decision. Such additional information is what we call phase 1 ID. In the IKE payload, there are local and peer ID field to achieve this.

## 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, IKE standard takes it as one type of Phase 1 ID.

Phase 1 ID is an identification for each VPN peer. The type of Phase 1 ID may be IP/FQDN(DNS)/User 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 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 Prestige, if "DNS" or "E-mail" type is chosen, you can still use a random string as the content, such as "this\_is\_Prestige". It's not necessary to follow the format exactly.

By default, Prestige takes IP as phase 1 ID type for itself and its remote peer. But if its remote peer is using DNS or E-mail, you have to adjust the settings to pass phase 1 ID checking.

## When should I use FQDN?

If your VPN connection is Prestige to Prestige, and both of them have static IP address, and there is no NAT router in between, you can ignore this option. Just leave Local/Peer ID type as IP, then skip this option.

If either side of VPN tunneling end point is using dynamic IP address, you may need to configure ID for the one with dynamic IP address. And in this case, "Aggressive mode" is recommended to be applied in phase 1 negotiation .

---

## Is my Prestige ready for IPSec VPN?

IPSec VPN is available for Prestige since ZyNOS V3.50. It is free upgrade, no registration is needed.

By upgrading the firmware and also configurations (romfile) to ZyNOS V3.50, the IPSec VPN capability



is ready in your Prestige. You then can configure VPN via web configurator. Please download the firmware from our web site.

NOTE: For updating from ZyNOS V3.2x to V3.5x, please use console or TFTP update. This is because the memory allocation difference between these two versions.

### **How do I configure Prestige VPN?**

You can configure Prestige for VPN using SMT or Web configurator. Prestige 1 supports Web only.

### **How many VPN connections does 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 by Prestige?**

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

### **What types of encryption does Prestige VPN support?**

Prestige supports 56-bit DES and 168-bit 3DES and AES.

### **What types of authentication does Prestige VPN 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 IP header of the packet (like the source/destination addresses), but ESP does not.

ESP can provide 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 go always 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 Prestige must have VPN capabilities. Please check the firmware version, V3.50 or later has the VPN capability.

If your Prestige is capable of VPN, you can find the VPN options in **Advanced>VPN** tab.

For configuring a 'box-to-box VPN', there are some tips:

1. If there is a NAT router running in the front of Prestige, please make sure the NAT router supports to pass through IPSec.
2. In NAT case (either run on the frond end router, or in Prestige VPN box), only IPSec ESP tunneling mode is supported since NAT againsts AH mode.
3. **Source IP/Destination IP**-- Please do not number the LANs (local and remote) using the same exact range of private IP addresses. This will make VPN destination addresses and the local LAN addresses are indistinguishable, and VPN will not work.
4. **Secure Gateway IP Address** -- This must be a public, routable IP address, private IP is not allowed. That means it can not be in the 10.x.x.x subnet, the 192.168.x.x subnet, nor in the range 172.16.0.0 - 172.31.255.255 (these address ranges are reserved by internet standard for private LAN numberings behind NAT devices). It is usually a static IP so that we can pre-configure it in Prestige for making VPN connections. If it is a dynamic IP given by ISP, you still can configure this IP address after the remote Prestige is on-line and its WAN IP is available from ISP.

### **Does Prestige support dynamic secure gateway IP?**

If the remote VPN gateways uses dynamic IP, we enter **0.0.0.0** as the **Secure Gateway IP Address** in Prestige. In this case, the VPN connection can only be initiated from dynamic side to fixed side in order to update its dynamic IP to the fixed side. However, if both gateways use dynamic IP addresses, it is no way to establish VPN connection at all.

### **What VPN gateway that has been tested with Prestige successfully?**

We have tested Prestige successfully with the following third party VPN gateways.

- 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

**What VPN software that has been tested with Prestige successfully?**

We have tested Prestige successfully with the following third party VPN software.

- 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, we will support it and we are working on it currently.

**Does Prestige VPN support NetBIOS broadcast?**

The current 3.50 firmware release does not support it. But it is in our wish list.

**Is the host behind NAT allowed to use IPsec?**

NAT Condition	Supported IPsec Protocol
VPN Gateway embedded NAT	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, for Prestige SUA/NAT routers, IPsec pass through is supported since ZyNOS 3.21. The default port and the client IP have to be specified in menu 15-SUA Server Setup.

**Why does VPN throughput decrease when staying in SMT menu 24.1?**

If Prestige stays in menu 24.1, 24.8 and 27.3 a certain of memory is allocated to generate the required statistics. So, we do not suggest to stay in menu 24.1, 27.3 and 24.8 when VPN is in use.

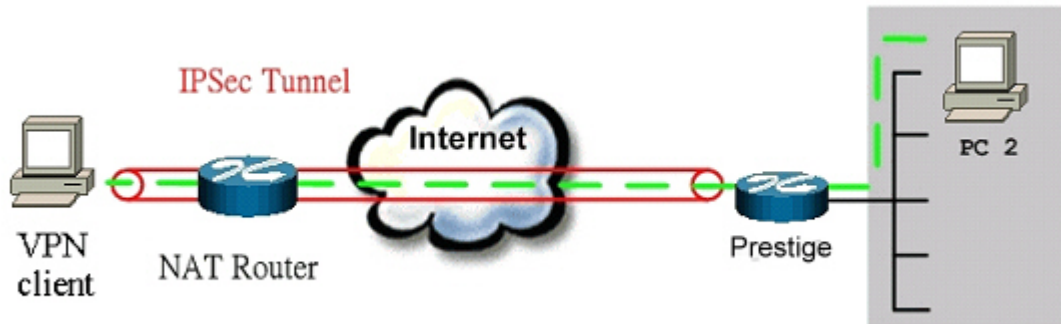
**Where can I configure Phase 1 ID in Prestige?**

Phase 1 ID can be configured in VPN setup menu as following. Note that you can make such configuration in either web configurator or SMT menu.

IPSec Key Mode	IKE
Negotiation Mode	Aggressive
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0
<b>Local</b>	
Local Address Type	Subnet
IP Address Start	<Prestige LAN>
End / Subnet Mask	255.255.255.0
<b>Remote</b>	
Remote Address Type	Subnet
IP Address Start	<Peer LAN>
End / Subnet Mask	255.255.255.0
<b>Address Information</b>	
Local ID Type	IP
Content	
My IP Address	0.0.0.0
Peer ID Type	E-mail
Content	<Sonicwall Serial #>
Secure Gateway Address	0.0.0.0

**If I have NAT router between two VPN gateways, and I would like to use IP type as Phase 1 ID, what should I know?**

We presume your environment may look like this,



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 case. This may cause the VPN client to send it's private IP address as the content of it's phase 1 ID. So you have to configure Prestige's secure gateway's phase 1 ID as the private IP address of the VPN client.

**How can I keep a tunnel alive?**

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

But to reduce the consumption of system resource, if VPN tunnels get disconnected either manually, by idle timer, or because of power cycle, packet triggering is still necessary to make the tunnel up.

**Single, Range, Subnet, which types of IP address do Prestige 10/10II/10W/50/100 support in VPN/IPSec?**

The mentioned Prestige series support all of the types. In other words, you can specify a single PC, a range of PCs or even a network of PCs to utilize the VPN/IPSec service.

**Can Prestige support IPSec passthrough?**

Yes, Prestige can support IPSec passthrough. Prestige series don't only support IPSec/VPN gateway, it can also be a NAT router supporting IPSec passthrough.

If the VPN connection is initiated from the security gateway behind Prestige, no configuration is necessary for NAT nor Firewall.

If the VPN connection is initiated from the security gateway outside of Prestige, NAT port forwarding and Firewall forwarding are necessary.

To configure NAT port forwarding, please go to WEB interface, **Setup/ "SUA/NAT"**, put the secure gateway's IP address in default server.

To configure Firewall forwarding, please go to WEB interface, **Setup/Firewall**, select Packet Direction to **WAN to LAN**, and create a firewall rule the forwards IKE(UDP:500).

### **Can Prestige behave as a NAT router supporting IPSec passthrough and an IPSec gateway simultaneously?**

No, Prestige can't support them simultaneously. You need to choose either one. If Prestige is to support IPSec passthrough, you have to disable the VPN function on Prestige. To disable it, you can either deactivate each VPN rule or issue a CI command, "**ipsec switch off**" from SMT menu 24.8. You can get into SMT menu via either telnet or console connection.

---

## **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 ether. Typical bit-rates are 11Mbps and 54Mbps, although in practice data throughput is half of this. Wireless LANs can be formed simply by equipping PC's with wireless NICs. If connectivity to a wired LAN is required an Access Point (AP) is used as a bridging device. AP's are typically located close to the centre of the wireless client population.

### **What are the advantages of Wireless LANs ?**

#### ***a. Mobility:***

Wireless LAN systems can 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 can eliminate the need to pull cable 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 wired LAN. The most popular wired LAN is operated in 100Mbps, which is almost 10 times of that of Wireless LAN (10Mbps). A faster wired LAN standard (1000Mbps), which is 100 times faster, becomes popular as well. The setup cost of Wireless LAN is relative high because the equipment cost including access point and PCMCIA Wireless LAN card is higher than hubs and CAT 5 cables.

**Where can you find wireless 802.11 networks ?**

Airports, hotels, and even coffee shops like Starbucks are deploying 802.11 networks so people can wirelessly browse the Internet with their laptops. As these types of networks increase, this will create additional security risk for the remote user if not properly protected.

**What is an Access Point ?**

The AP (access point also known as a base station) is the wireless server that with an antenna and a wired

Ethernet connection that broadcasts information using radio signals. AP typically act as a bridge for the clients. It can pass information to wireless LAN cards that have been installed in computers or laptops allowing those computers to connect to the campus network and the Internet without wires.

### **What is IEEE 802.11 ?**

The 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. 802.11 provides 1 or 2 Mbps transmission in the 2.4 GHz ISM band using either FHSS or DSSS.

### **What is 802.11b ?**

802.11b is the first revision of 802.11 standard allowing data rates up to 11Mbps in the 2.4GHz ISM band. Also known as 802.11 High-Rate and Wi-Fi. 802.11b only uses DSSS, the maximum speed of 11Mbps has fallbacks to 5.5, 2 and 1Mbps.

### **How fast is 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 other people are using the wireless ethernet 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 802.11a ?**

802.11a the second revision of 802.11 that operates in the unlicensed 5 GHz band and allows transmission rates of up to 54Mbps. 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., 802.11b and 802.11g) and can increase the cost of the overall solution because a greater number of access points may be required. 802.11a is not directly compatible with 802.11b or 802.11g networks. In other words, a user equipped with an 802.11b or 802.11g radio card will not be able to interface directly to an 802.11a access point. Multi-mode NICs will solve this problem.

### **What is 802.11g ?**

802.11g is an extension to 802.11b. 802.11g increases 802.11b's data rates to 54 Mbps and still utilise the 2.4 GHz ISM. Modulation is based upon OFDM (orthogonal frequency division multiplexing)



technology. An 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. The range at 54 Mbps is less than for 802.11b operating at 11 Mbps.

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

Yes. As long as the products comply to the same IEEE 802.11 standard. The Wi-Fi logo is used to define 802.11b compatible products. Wi-Fi5 is a compatibility standard for 802.11a products running in the 5GHz band.

### **What is Wi-Fi ?**

The Wi-Fi logo signifies that a product is interoperable with wireless networking equipment from other vendors. A Wi-Fi logo product has been tested and certified by the Wireless Ethernet Compatibility Alliance (WECA). The Socket Wireless LAN Card is Wi-Fi certified, and that means that it will work (interoperate) with any brand of Access Point 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 802.11 interfere with Bluetooth devices ?**

Any time devices are operated in the same frequency band, there is the potential for interference. Both the 802.11b and Bluetooth devices occupy the same 2.4-to-2.483-GHz unlicensed frequency range-the same band. But a Bluetooth device would not interfere with other 802.11 devices much more than another 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 802.11 device, or a new 2.4 GHz cordless phone for that matter. But, Bluetooth devices are usually low-power, so the effects that a Bluetooth device may have on an 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 are potential factors that may causes 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 setting. 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. Without using an access point or any connection to a wired network.

### **What is Infrastructure mode ?**

Infrastructure mode implies connectivity to a wired communications infrastructure. If such connectivity is required the Access Points must be used to connected to the wired LAN backbone. Wireless clients have their configurations set for "infrastructure mode" in order to utilise access points relaying.

**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 extend coverage.

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

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 Frequency-hopping Spread Spectrum Technology – (FHSS) ?**

FHSS uses a narrowband carrier which hops through a predefined sequence of several frequencies at a specific rate. This avoids problems with fixed channel narrowband noise and simple jamming. Both transmitter and receiver must have their hopping sequences synchronized to create the effect of a single "logical channel". To an unsynchronised receivers an FHSS transmission appears to be short-duration impulse noise. 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 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 radios 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 Server Set ID (SSID) ?**

SSID is a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. SSID from a security point of view acts as a simple single shared password between base stations and clients.

### **What is an ESSID ?**

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

### **How do I secure the data across an Access Point's radio link ?**

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

### **What is WEP ?**

Wired Equivalent Privacy. WEP is a security mechanism defined within the 802.11 standard and designed to make the security of the wireless medium equal to that of a cable (wire). WEP data encryption was designed to prevent access to the network by "intruders" and to prevent the capture of wireless LAN traffic through eavesdropping. WEP allows the administrator to define a set of respective "Keys" for each wireless network user based on a "Key String" passed through the WEP encryption algorithm. Access is denied by anyone who does not have an assigned key. WEP comes in 40/64-bit and 128-bit encryption key lengths. Note, WEP has shown to have fundamental flaws in its key generation processing.

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

40 bit WEP & 64 bit WEP are the same encryption level and can interoperate. The lower level of WEP encryption uses a 40 bit (10 Hex character) as "secret key" (set by user), and a 24 bit " Initialization Vector " (not under user control) (40+24=64). Some vendors refer to this level of WEP as 40 bit, others as 64 bit.

### **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 ?**

128-bit WEP will not communicate with 64-bit WEP or 256-bit WEP. Although 128 bit WEP also uses a 24 bit Initialization Vector, but it uses a 104 bit as secret key. Users need to use the same encryption level in order to make a connection.

**Can the SSID be encrypted ?**

WEP, the encryption standard for 802.11, only encrypts the data packets not the 802.11 management packets and the SSID is in the beacon and probe management messages. The SSID is not encrypted if WEP is turned on. The SSID goes over the air in clear text. This makes obtaining the SSID easy by sniffing 802.11 wireless traffic.

**By turning off the broadcast of SSID, can someone still sniff the SSID ?**

Many APs by default have broadcasting the SSID turned on. Sniffers typically will find the SSID in the broadcast beacon packets. Turning off the broadcast of SSID in the beacon message (a common practice) does not prevent getting the SSID; since the SSID is sent in the clear in the probe message when a client associates to an AP, a sniffer just has to wait for a valid user to associate to the network to see the SSID.

**What are Insertion Attacks ?**

The insertion attacks are based on placing unauthorized devices on the wireless network without going through a security process and review.

**What is Wireless Sniffer ?**

An attacker can sniff and capture legitimate traffic. Many of the sniffer tools for Ethernet are based on capturing the first part of the connection session, where the data would typically include the username and password. An intruder can masquerade as that user by using this captured information. An intruder who monitors the wireless network can apply this same attack principle on the wireless.

**What is the difference between Open System and Shared Key of Authentication Type ?**

Open System:

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 designates open system authentication.

Share Key:

The optional authentication 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 802.1x ?**

IEEE 802.1x Port-Based Network Access Control is an IEEE (Institute of Electrical and Electronics Engineers) standard, which specifies a standard mechanism for authenticating, at the link layer (Layer 2), users' access to IEEE 802 networks such as Ethernet (IEEE 802.3) and Wireless LAN (IEEE 802.11). For IEEE 802.11 WLAN, IEEE 802.1x authentication can be based on username/password or digital certificate.

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

No authentication required—disables 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 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 switch cannot provide authentication services to the client through the interface.

Authentication required—enables 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 switch 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 switch by using the client's MAC address.

### **What is AAA ?**

AAA is the acronym for Authentication, Authorization, and Accounting and 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 name and password or MAC address) and accounting for their network usage.

### **What is RADIUS ?**

RADIUS stands for Remote Authentication Dial-In User Service. RADIUS 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 wireless AP/gateway and wireless client. As long as the passwords match, a client will be granted access to the WLAN.

---

## **Trouble Shooting**

For general device installation or basic trouble shooting please refer to the device user's guide

### **Using Embedded Packet Trace**

#### [Embedded Packet Trace](#)

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

The format of the display is as following:

Packet:

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

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

There are two ways to dump the trace:

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

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

### Online Trace

1. Trace LAN packet
  2. Trace WAN packet
- 

1. Trace LAN packet

- 1.1 Disable to capture the WAN packet by entering: **sys trcp channel enet1 none**
  - 1.2 Enable to capture the LAN packet by entering: **sys trcp channel enet0 bothway**
  - 1.3 Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
  - 1.4 Display the brief trace online by entering: **sys trcd brief**
- or
- 1.5 Display the detailed trace online by entering: **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 ENETO-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
 1  11883.100 ENETO-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
 2  11883.330 ENETO-T[0058] TCP 192.31.7.130:80->192.168.1.2:1108
 3  11883.340 ENETO-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
 4  11883.340 ENETO-R[0339] TCP 192.168.1.2:1108->192.31.7.130:80
 5  11883.610 ENETO-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
 6  11883.620 ENETO-T[0102] TCP 192.31.7.130:80->192.168.1.2:1108
```



```
7 11883.630 ENETO-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
8 11883.630 ENETO-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
9 11883.650 ENETO-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
10 11883.650 ENETO-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80
```

```
Prestige> sys trcd parse
```

```
---<0000>-----
```

```
LAN Frame: ENETO-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: ENETO-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: ENETO-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 to capture the LAN packet by entering: **sys trcp channel enet0 none**
  - 1.2 Enable to capture the WAN packet by entering: **sys trcp channel enet1 bothway**
  - 1.3 Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
  - 1.4 Display the brief trace online by entering: **sys trcd brief**
- or
- 1.5 Display the detailed trace online by entering: **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 to capture the WAN packet by entering: `sys trcp channel enet1 none`
- 1.2 Enable to capture the LAN packet by entering: `sys trcp channel enet0 bothway`
- 1.3 Enable the trace log by entering: `sys trcp sw on` & `sys trcl sw on`
- 1.4 Wait for packet passing through Prestige over LAN
- 1.5 Disable the trace log by entering: `sys trcp sw off` & `sys trcl sw off`
- 1.6 Display the trace briefly by entering: `sys trcp brief`
- 1.7 Display specific packets by using: `sys trcp parse <from_index> <to_index>`

### Exmample:

```
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 ENETO-R[0060] TCP 192.168.1.2:1103->192.31.7.130:80
```

```
Prestige> sys trcp parse 5 5
```

```
---<0005>-----
```

```
LAN Frame: ENETO-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 to capture the LAN packet by entering: **sys trcp channel enet0 none**
- 1.2 Enable to capture the WAN packet by entering: **sys trcp channel enet1 bothway**
- 1.3 Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
- 1.4 Wait for packet passing through Prestige over WAN
- 1.5 Disable the trace log by entering: **sys trcp sw off & sys trcl sw off**
- 1.6 Display the trace briefly by entering: **sys trcp brief**
- 1.7 Display specific packets by using: **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>

```

**Debug PPPoE Connection**

**Debug PPPoE Connection**

The Prestige supports traces when there is problem to connect your ISP using PPPoE protocol. Please follow the procedure below to collect the trace for our troubleshooting.

1. Remove the LAN cable attached on the Prestige
2. Enter SMT using console port
3. Enter 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 enter debug mode after the crash)
  - `poe debug 1` (turn on pppoe debug)
  - `dev dial 1` (dial remote node 1)
5. After all, if the Prestige crashes and you can do nothing, please send the above log back to us.
6. If the Prestige crashes and you are able to enter commands, please type 'atds' in debug mode to dump the log and send the log to us.
7. If the Prestige does not crash but just can not dial out, please capture the following further log and send us the log.
  - `sys trcp sw off` (turn off packet trace)
  - `sys log disp i` (capture system error log)
  - `sys trcp parse` (parse the trace in detail)

---

### **Example- A trace with system crashes**

```
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
poePut1SrvName: '' len 0
host-uniq 31303030 len 4
```

```
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
bdcastSendInit: ll.pktTx() failed, pch poe0 ch enet0
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0.....
poeI/C: ver 1 type 1 code x07 sessId x0000 len 274(x0112)
poeCtrlI/C: pkt len 274
poeGetTags()
service-name
service-name telstra
service-name bpa
service-name iprimus
service-name pacificinternet
service-name integrationisp
service-name bpa-dev
service-name bpa-sif
service-name telstrarna
service-name gpmsystems
service-name cmux
service-name launceston-broadband
service-name vivanet
service-name n1234567k00
service-name bigpond
service-name n7061992k
service-name n3068223k
service-name n2155202k
service-name n7061995k
AC-name vet1-exhibition-bsn-1
host-uniq 31303030 len 4
PADO recv'd, chann enet1
procPADO: for poe chann poe0
Chann poe0 sending request
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x19 sess-id 0 len 12(x000C)
```



Undefined Address : 0xE3F045C4

Undefined Data : 0x56FF54FF

r0= 0xE3F045C4	r1= 0x0001FFC0	r2= 0x000000E5	r3= 0x56FF54FF
r4= 0xE3F045C4	r5= 0xE5BDBFEC	r6= 0x0001C468	r7= 0x60000093
r8= 0x00000000	r9= 0xE3550000	r10=0xE3550000	fp= 0x00000000
r12=0x56FF54FF	sp= 0x0001EDBC	lr= 0x00004F64	pc= 0x00013954

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

```

e5bdbfe0: e2 8f 00 06 e5 d5 20 06 e5 d5 20 0a e5 d5 20 0e ...b...f...j...n
e5bdbff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc000: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc010: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc020: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc030: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc040: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc050: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc060: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc070: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc080: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc090: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n

```

Bootbase Version: V1.10 | 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 P2602R, 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

---

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

The format of the display is as following:

Packet:

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

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

There are two ways to dump the trace:

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

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

### Online Trace

1. Trace LAN packet
  2. Trace WAN packet
-

## 1. Trace LAN packet

- 1.1 Disable to capture the WAN packet by entering: **sys trcp channel mpoa00 none**
  - 1.2 Enable to capture the LAN packet by entering: **sys trcp channel enet0 bothway**
  - 1.3 Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
  - 1.4 Display the brief trace online by entering: **sys trcd brief**
- or
- 1.5 Display the detailed trace online by entering: **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  11883.2602HWL ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
10  11883.2602HWL 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 (2602HWL40)  
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: ENETO-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 the capture of the LAN packet by entering: **sys trcp channel enet0 none**
  - 1.2 Enable to capture the WAN packet by entering: **sys trcp channel mpoa00 bothway**
  - 1.3 Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
  - 1.4 Display the brief trace online by entering: **sys trcd brief**
- or
- 1.5 Display the detailed trace online by entering: **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 (2602HWL40)
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 the capture of the WAN packet by entering: **sys trcp channel mpoa00 none**
- 1.2 Enable the capture of the LAN packet by entering: **sys trcp channel enet0 bothway**
- 1.3 Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
- 1.4 Wait for packet passing through the Prestige over LAN
- 1.5 Disable the trace log by entering: **sys trcp sw off & sys trcl sw off**
- 1.6 Display the trace briefly by entering: **sys trcp brief**
- 1.7 Display specific packets by using: **sys trcp parse <from\_index> <to\_index>**

### 2. Trace WAN packet

- 1.1 Disable the capture of the LAN packet by entering: **sys trcp channel enet0 none**
- 1.2 Enable the capture of the WAN packet by entering: **sys trcp channel mpoa00 bothway**
- 1.3 Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
- 1.4 Wait for packet passing through the Prestige over WAN
- 1.5 Disable the trace log by entering: **sys trcp sw off & sys trcl sw off**
- 1.6 Display the trace briefly by entering: **sys trcp brief**
- 1.7 Display specific packets by using: **sys trcp parse <from\_index> <to\_index>**

## CLI Command List

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