P334WT Support Note

V360(JN0)
Last Update: October 8, 2004

ZyNOS FAQ

---

1. What is ZyNOS?

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

2. How do I access the Prestige SMT menu?

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

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

The default console port baud rate is 9600bps, you can change it to 115200bps in Menu 24.2.2 to

speed up the SMT access.

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

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

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

The procedure for uploading Prestige via console is as follows.

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

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

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

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

6. How do I upload ROMFILE via console port?

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

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

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

7. How do I backup/restore SMT configurations by using TFTP client program via LAN?

a. Use the TELNET client program in your PC to login to your Prestige.
b. Enter CI command **'sys stdio 0'** in menu 24.8 to disable console idle timeout.

c. To backup the SMT configurations, use TFTP client program to get file '**rom-0**' from the Prestige.
d. To restore the SMT configurations, use the TFTP client program to put your configuration in file **rom-0** in the Prestige.

8. Why can't I make Telnet to Prestige from WAN?

There are three reasons that Telnet from WAN is blocked.

1. You have disabled Telnet service in Menu 24.11.

   Source IP= Telnet host
   Destination IP= Prestige's WAN IP
   Service= TCP/23
   Action=Forward

2. Telnet service is enabled but your host IP is not the securied host entered in Menu 24.11. In this case, the error message ***'Client IP is not allowed!'*** is appeared on the Telnet screen.
3. The filter rule is applied in the Input Protocol field in menu 11.5 to block Telnet service.
4. The console port is in use.

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

In case you forget the system password, you need to upload ROMFILE to reset the SMT to factory default. After uploading ROMFILE, the default system password is '**1234**'.

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

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

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

11. 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.

12. 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 334WT supports 2048 sessions that you can use the **'ip nat iface enif1'** command in menu 24.8 to view the current active sessions.

13. 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'.

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

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

15. How can I protect against IP spoofing attacks?

The P334WT'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.

Product FAQ

General FAQ

1. What is the P334WT Internet Access Sharing Router?
2. Will the P334WT work with my Internet connection?
3. What do I need to use the Prestige?
4. What is PPPoE?
5. Does the Prestige support PPPoE?
6. How do I know I am using PPPoE?
7. Why does my provider use PPPoE?
8. Which Internet Applications can I use with the Prestige?
9. How can I configure the Prestige?
10. What network interface does the Prestige support?
11. What can we do with Prestige?
12. Does Prestige support dynamic IP addressing?
13. What is the difference between the internal IP and the real IP from my ISP?
14. How does e-mail work through the Prestige?
15. What is the main difference between WinGate and the Prestige?
16. What is the difference between the 'Standard' and 'RoadRunner' service?
17. Is it possible to access a server running behind SUA from the outside Internet? If possible, how?
18. What DHCP capability does the Prestige support?
19. What to do when Prestige response nothing via Console?
20. What network interface does the new Prestige series support?

Advanced FAQ

1. How does the Prestige support TFTP?
2. Can the Prestige support TFTP over WAN?
3. How can I upload data to outside Internet over the one-way cable?
4. How fast can the data go?
5. My Prestige can not get an IP address from the ISP to connect to the Internet, what can I do?
6. How do I make VPN client x work through my Prestige?
7. What is Multi-NAT?
8. When do I need Multi-NAT?
9. What IP/Port mapping does Multi-NAT support?
10. What is the difference between SUA and Multi-NAT?

---

1. What is the P334WT Internet Access Sharing Router?

The Prestige series fulfills a range of application environments, from small and medium businesses, SOHO, or Telecommuters, to home user or education applications. The Prestige series provides a robust Firewall to protect your network. 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 your cable or ADSL modem. The router equipped with 1 auto-MDI/MDIX 10/100Mbps Ethernet WAN port and 4 auto-MDI/MDIX 10/100Mbps Etherent LAN port.

Virtually all-popular applications over Internet, such as Web, E-Mail, FTP, Telnet, Gopher, are supported.

2. Will the P334WT work with my Internet connection?

The P334WT is designed to be compatible with cable and ADSL modems. Most external Cable and ADSL modems use an Ethernet port to connect to your computer so the Prestige is placed in the line between the computer and the External modem. As long as your Internet Access device has an Ethernet port, you can use the Prestige. Besides, if your ISP supports PPPoE you can also use the Prestige, because PPPoE had been supported in the Prestige.

3. What do I need to use the Prestige?

You need a ADSL modem or cable modem with an Ethernet port to use the Prestige. The Prestige has two Ethernet ports: LAN port and WAN port. You should connect the computer to the LAN port and connect the external modem to the WAN port. If the ISP uses PPPoE or RoadRunner Authentication you need the user account to enter in the Prestige.

4. What is PPPoE?

PPPoE stands for **P**oint-to-**P**oint **P**rotocol **O**ver **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.

5. Does the Prestige support PPPoE?

Yes. The Prestige supports PPPoE.

6. How do I know I am using PPPoE?

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

7. Why does my provider use PPPoE?

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

8. Which Internet Applications can I use with the Prestige?

Most common applications includes MIRC, PPTP, ICQ, Cu- SeeMe, NetMeeting, IP/TV, RealPlayer, VDOLive, Quake, Quake11, Quake111, StarCraft, & Quick Time.

9. How can I configure the Prestige?

- Using Console connection-Menu driven user interface for easy local management
- Telnet remote management- Menu driven user interface for easy remote management
- Web broswer- web server embedded for easy configurations

10. What network interface does the Prestige support?

The Prestige supports 10/100M Ethernet to connect to the computer and 10M Ethernet to connect to the external cable or ADSL modem..

11. 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.

12. Does Prestige support dynamic IP addressing?

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

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

Internal IPs are 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 routes between the virtual IP and the real IP.

14. 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 Sharing Router 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.

15. What is the main difference between WinGate and the Prestige?

1. WinGate is a software only solution that needs to be installed in a dedicated Windows 95 PC based server. The total cost and complexity are many times over ATI’s product. The Prestige Internet Access Sharing Router is a plug-n-play internet appliance.
2. WinGate requires all TCP/IP applications such as Netscape Navigator to be reconfigured to have the dedicated server as a proxy. The Prestige Internet Access Sharing Router does not require users to reconfigure any software at all.
3. The Prestige Internet Access Sharing Router uses Network Address Translation (NAT)

scheme, which supports all TCP/UDP ports. WinGate only supports limited number of ports, such as http(80), ftp(21), telnet(23), and pop3(110).

4. WinGate works as a proxy, while the Prestige Internet Access Sharing Router works as a gateway. The gateway approach is more efficient than the proxy during the processing of TCP/IP commands. As a result, the Prestige Internet Access Sharing Router achieves 10% to 20% higher performance than that of software solutions such as WinGate.
5. The Prestige Internet Access Sharing Router uses Solid State Disk technology. There are no moving parts in the product. It is much more reliable than any hard disk based system, such as the one for WinGate.

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

The US **Road Runner** service requires the user to "log in" to the service before it can send any packets to the outside network. This is apparently implemented in the TAS (Toshiba Authentication System) with a packet filtering firewall in the upstream direction. Before login, one can send ICMP packets (e.g., ping) to the outside Internet, but nearly all other upstream TCP and UDP packets are blocked. The user can only speak to the local DNS/login server. Downstream packets do not appear to be filtered or blocked at any time.

While **Standard** service means the cable services which have no login requirement. Prestige supports both **Road Runner & Standard** services in menu 4 for connecting to cable ISPs.

17. 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**.

18. What DHCP capability does the Prestige support?

The Prestige supports DHCP client on the WAN port and DHCP server on the LAN port. The Prestige's DHCP client allows it to get the Internet IP address from ISP automatically. The Prestige's DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

19. What to do when when Prestige response nothing via console ?

When Prestige responses nothing on your terminal (e.g. embedded HyperTerminal), please try following methods

1. Make sure the CON/AUX (which is close to the power jet) switch of P334WT is set to CON, not AUX.

2. Please check whether RS-232 cable is well connected between Prestige and your computer.

3. Please try any baud rate between 9600 bps to 115200 bps in case the baud has been changed.

20. What network interface does the new Prestige series support?

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

Advanced FAQ

1. 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.

2. 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.

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

A workaround is to use an alternate path for your upstream path, such as a dialup connection to an Internet service provider. So, if you can find another way to get your upstream packets to the Internet you will still be able to receive downstream packets via Prestige.

4. How fast can the data go?

The speed of the cable modem 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.

5. My Prestige can not get an IP address from the ISP to connect to the Internet, what can I do?

Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use three ways:

1. Check if the 'MAC address' is valid

2. Check if the 'Host Name' is valid, e.g., @home

3. Check if the 'User ID' is valid, e.g., RR-Toshiba Authentication Service, RR-Manager Authentication Service

If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for the authentication. So, if a new network card is used or the Prestige is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP.

The Prestige supports to clone the MAC from the first PC the ISP installed to be its WAN MAC. To clone the MAC from the PC you need to enter that PC's IP in menu 2. Once the MAC is received by

the Prestige, the WAN MAC in menu 24.1 will be updated and used for the ISP's authentication.

```
Menu 2 - WAN Setup

Link Mode= Half Duplex

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

Key settings:

- Assigned By, Choose **'IP address attached on LAN'.**
- IP Address, Enter the IP address of the PC which is installed by the ISP at the first installation.

2. Your ISP checks the 'Host Name'

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. When first installing, the ISP's tech people configure the host name as the 'Computer Name' of the PC in the 'Networking' settings. When the Prestige is attached to the cable modem to connect to the ISP, we should configure this host name in the Prestige's system (menu 1).

```
Menu 1 - General Setup

System Name= zyxel
```

Key Setting:

- System Name=, The system name must be the same as the PC's computer name.

3. Your ISP checks 'User ID'

This authentication type is used by RoadRunner ISP, currently they use RR-TAS(Toshiba Authentication Service) and RR-Manager authentications. You must configure the correct 'Service Type', username and password for your ISP in menu 4.

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Service Type= RR-Toshiba Authentication Service
Server IP= 0.0.0.0
My Login=
My Password= ********

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
RIP Direction= None
Version= N/A
Single User Account= Yes
Edit Filter Set= No


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

Key settings:

- Service Type.....Currently, there are two authentication types that Road Runner supports, **RR-TAS** and **RR-Manager.** Choose the correct one for your local ISP.
- Server IP.....The Prestige will find the Road Runner server IP if this field is blank, otherwise enter the authentication server IP address if you know it.
- My Login Name...Enter the login name given to you by your ISP
- My Password.....Enter the password associated with the login name
- WAN IP Address Assignment...If the ISP did not assign you an explicit IP, select **Dynamic**, otherwise, select **Static**.
- IP Address & Subnet Mask & Gateway IP Address...Enter the IP address, subnet mask & gateway IP when **Static** Assignment is selected above.

6. How do I make VPN client x work through my Prestige?

The only VPN known for certain to work through the Prestige is Microsoft PPTP.

7. 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)*.

8. When do I need Multi-NAT?

- Make local server accessible from outside Internet

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

- Support Non-NAT Friendly Applications

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

9. 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

10. 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 severs of the same type (e. g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions that supported SUA 'visible' servers had to be of different types. The 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.

11. 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.

12. 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.

Without DDNS, we always tell the users to use the WAN IP of the Prestige 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 Prestige.

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.

13. 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.

14. What DDNS servers does the Prestige support?

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

15. 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.

16. Does the Prestige support DDNS wildcard?

Yes, the Prestige supports DDNS wildcard that WWW.DynDNS.ORG supports. When using wildcard, you simply enter yourhost.dyndns.org in the **Host** field in Menu 1.1.

17. Can the Prestige SUA handle IPsec packets sent by the IPsec gateway?

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.

18. 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.

19. Why can't I use video conferencing with MSN 4.6?

This is because MSN 4.6 require support of UPnP (Universal plug n’ play). To be able to use MSN through Prestige, you have to enable the UPnP feature under Advanced-> UPNP and Check the enable UPnP check box and press "Apply button" to make it active.

20. How can I access internal server via public IP address assigned on WAN?

You should be able to access your internal server via it's internal IP address when SUA is on, to access your internal server via the public IP address assigned on WAN, you can enter CI command "**ip nat loopback on**" in SMT Menu 24.8, To make the configuration permanently, you need to add this command to the system boot file (autoexec.net). You can refer to Product Support Note section on www.zyxel.com for configuration details.

21. Should I create any firewall rule by myself to allow incoming traffic when NAT is used ?

Built-in firewall function is supported in P334WT. When a session is initiated from a user located in

P334WT's LAN network, incoming traffic will be allowed by Stateful Inspection mechanism. However, if the session is initiated from WAN side and there is no related access rule for the incoming traffic, the traffic will be blocked by P334WT. To help users get rid of the problem and configuration tasks, P334WT will create firewall policy automatically to allow incoming traffic if NAT is enabled in the P334WTs. Following NAT types ,including: Port Mapping, One-to-one, Many one-to-one, Server Type are supported with automatic ACL rule creation function for incoming traffic. Therefore, users don't have to configure any access rule by themselves to support FTP, WEB, TELNET ...etc services.

General

---

1. 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.

2. What makes P334WT secure?

The P334WT 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 P334WT 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.

3. 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.

4. What kind of firewall is the P334WT?

1. The P334WT'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 P334WT'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 P334WT'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 P334WT'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 P334WT's firewall provides email service to notify you for routine reports and when alerts occur.

5. 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.

6. 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

7. 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.

8. 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.

9. 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.

10. 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.

11 What is Brute-force attack?

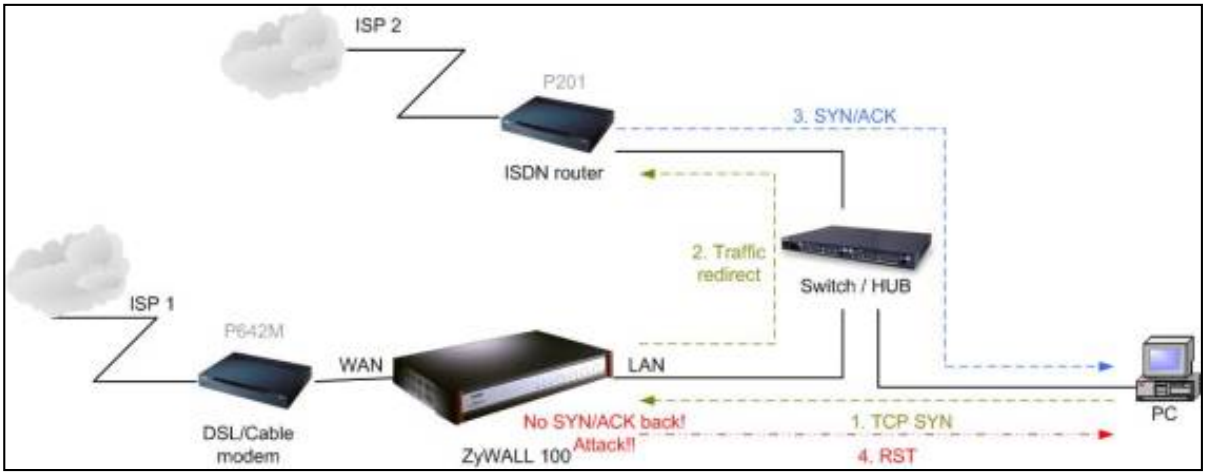
A Brute-force attack, such as 'Smurf' attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address of each packet is the broadcast address of the network, the router will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

12. 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.

13. Why traffic redirect/static/policy route be blocked by P334WT?

P334WT is a secure gateway for all data passing between the Internet and the LAN. For some reasons (load balance or backup line), users may want traffic to be re-routed to another Internet access devices while still be protected by Prestige. In such case, the network topology is the most important issue. Here is a common example that people mis-deploy the LAN traffic redirect and static route.



The above figure indicates the "**triangle route**" topology. It works fine if you turn off firewall function on P334WT box. By default, your connection will be blocked by firewall because of the following reason.

Step 1. Being the default gateway of PC, P334WT will receive all "outgoing" traffic from PC.

Step 2. And because of **Static route/Traffic Redirect/Policy Routing**, P334WT forwards the traffic to another gateway (ISDN/Router) which is in **the same segment** as P334WT's

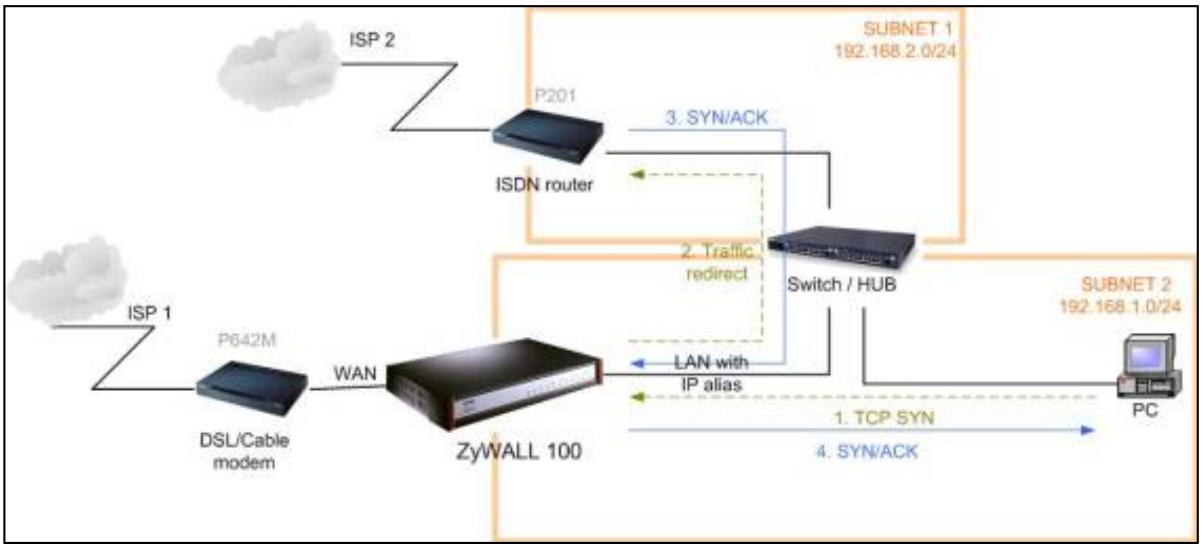
LAN.

Step 3. However the return traffic won't go back to P334WT, in stead, the "another gateway (ISDN/Router)" will send back the traffic to PC directly. Because the gateway (say, P201) and the PC are in the same segment.

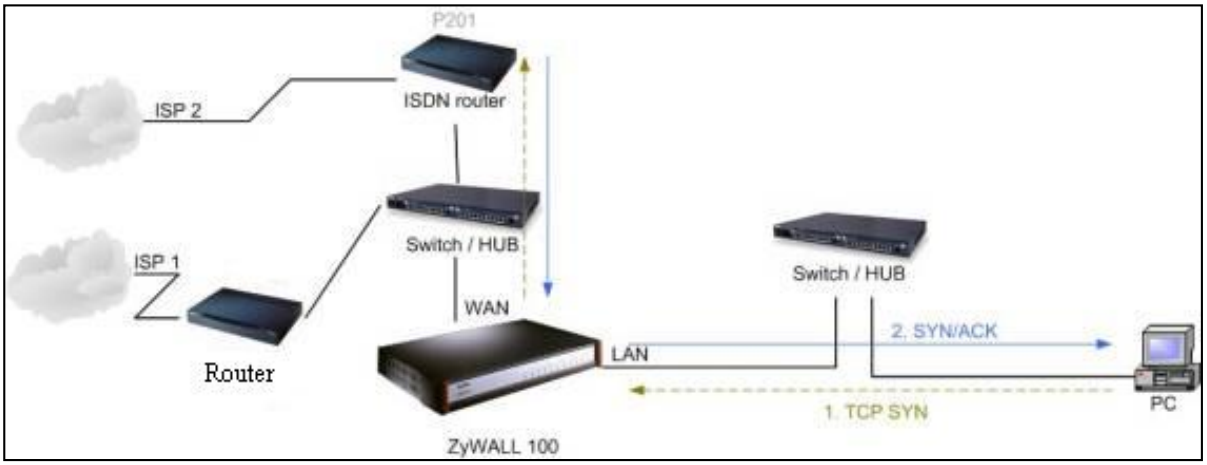
By default, P334WT will check the outgoing traffic by ACL and create dynamic sessions to allow return traffic to go back. To achieve Anti-DoS, P334WT will send RST packets to the PC and the peer since it never receives the TCP SYN/ACK packet. Thus the connection will always be reset by P334WT.

Solutions.

(A) Deploying your second gateway in IP alias segment is a better solution. In this way, your connection can be always under control of firewall. And thus there won't be Triangle Route problem.



(B) Deploying your second gateway on WAN side.



(C) To resolve this conflict, we add an option for users to allow/disallow such **Triangle Route** topology in both CI command and Web configurator . You can issue this command, "**sys firewall ignore triangle all on**" , to allow firewall bypass triangle route checking. In Web GUI, you can find this option in firewall setup page.

But we would like to notify that if you allow Triangle Route, any traffic will be easily injected into the protected network through the unprotected gateway. In fact, it's a security hole in protected your network.

General

---

1. 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.

2. What makes P334WT secure?

The P334WT 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 P334WT 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.

3. 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.

4. What kind of firewall is the P334WT?

1. The P334WT'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 P334WT'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 P334WT'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 P334WT'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 P334WT's firewall provides email service to notify you for routine reports and when alerts occur.

5. 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.

6. 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

7. 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.

8. 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.

9. 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.

10. 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.

11 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

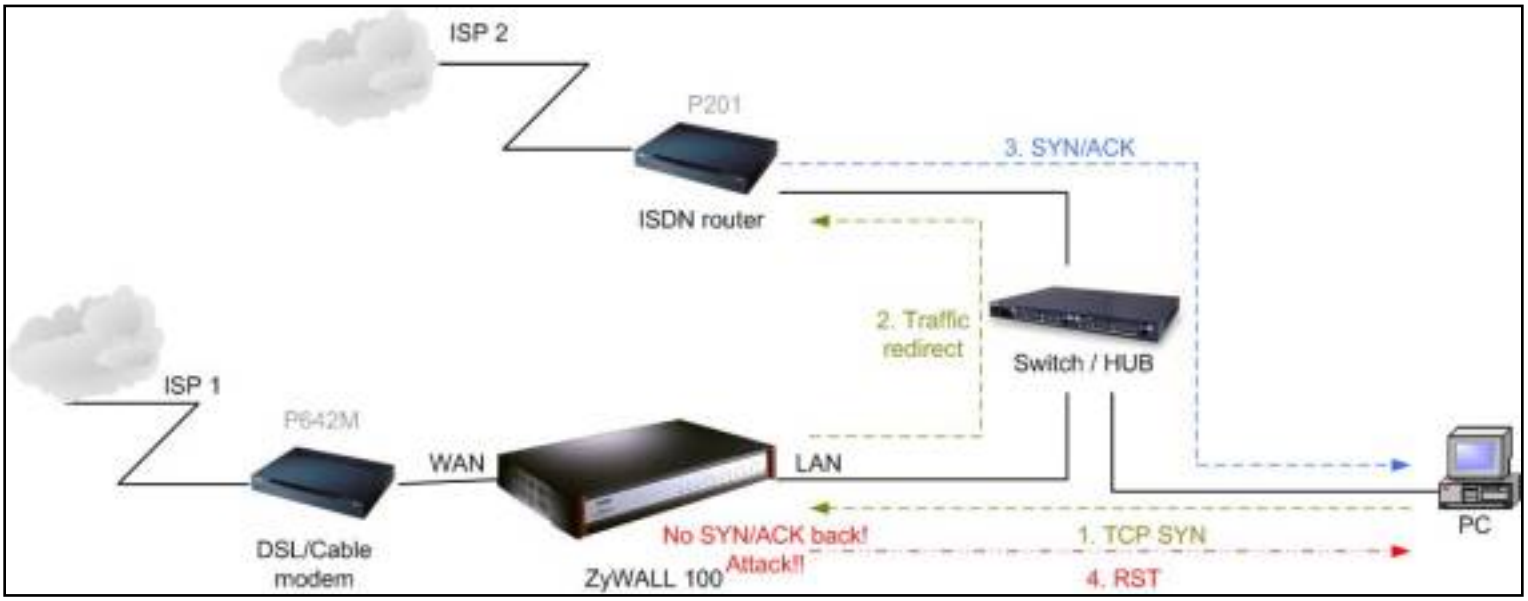
will create a large amount of ICMP echo request packet, the resulting ICMP traffic will not only clog up the 'intermediary' network, but will also congest the network of the spoofed source IP address, known as the 'victim' network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

12. 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.

13. Why traffic redirect/static/policy route be blocked by P334WT?

P334WT is a secure gateway for all data passing between the Internet and the LAN. For some reasons (load balance or backup line), users may want traffic to be re-routed to another Internet access devices while still be protected by Prestige. In such case, the network topology is the most important issue. Here is a common example that people mis-deploy the LAN traffic redirect and static route.



The above figure indicates the "**triangle route**" topology. It works fine if you turn off firewall function on P334WT box. By default, your connection will be blocked by firewall because of the following reason.

Step 1. Being the default gateway of PC, P334WT will receive all "outgoing" traffic from PC.

Step 2. And because of **Static route/Traffic Redirect/Policy Routing**, P334WT forwards

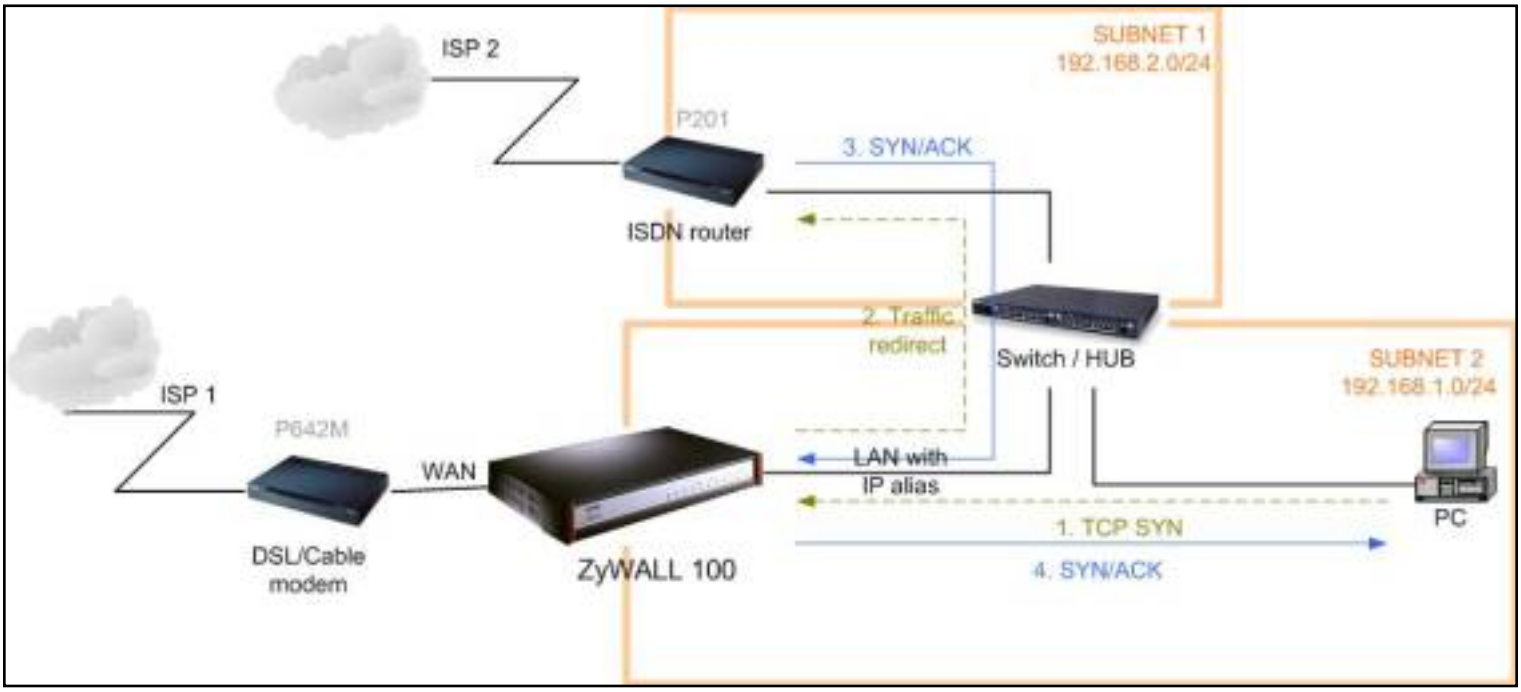
the traffic to another gateway (ISDN/Router) which is in **the same segment** as P334WT's LAN.

Step 3. However the return traffic won't go back to P334WT, in stead, the "another gateway (ISDN/Router)" will send back the traffic to PC directly. Because the gateway (say, P201) and the PC are in the same segment.

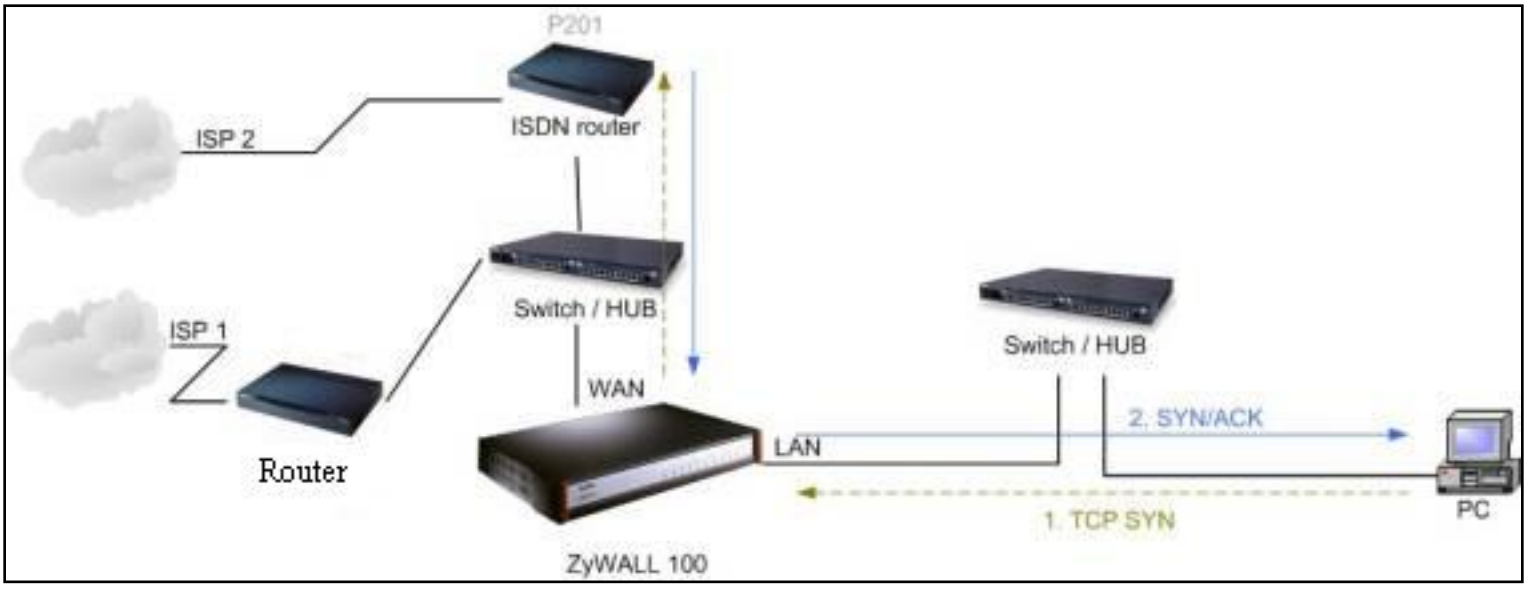
By default, P334WT will check the outgoing traffic by ACL and create dynamic sessions to allow return traffic to go back. To achieve Anti-DoS, P334WT will send RST packets to the PC and the peer since it never receives the TCP SYN/ACK packet. Thus the connection will always be reset by P334WT.

Solutions.

(A) Deploying your second gateway in IP alias segment is a better solution. In this way, your connection can be always under control of firewall. And thus there won't be Triangle Route problem.



(B) Deploying your second gateway on WAN side.



(C) To resolve this conflict, we add an option for users to allow/disallow such **Triangle Route** topology in both CI command and Web configurator . You can issue this command, "**sys firewall ignore triangle all on**" , to allow firewall bypass triangle route checking. In Web GUI, you can find this option in firewall setup page.

But we would like to notify that if you allow Triangle Route, any traffic will be easily injected into the protected network through the unprotected gateway. **In fact, it's a security hole in protected your network.**

Log and Alert

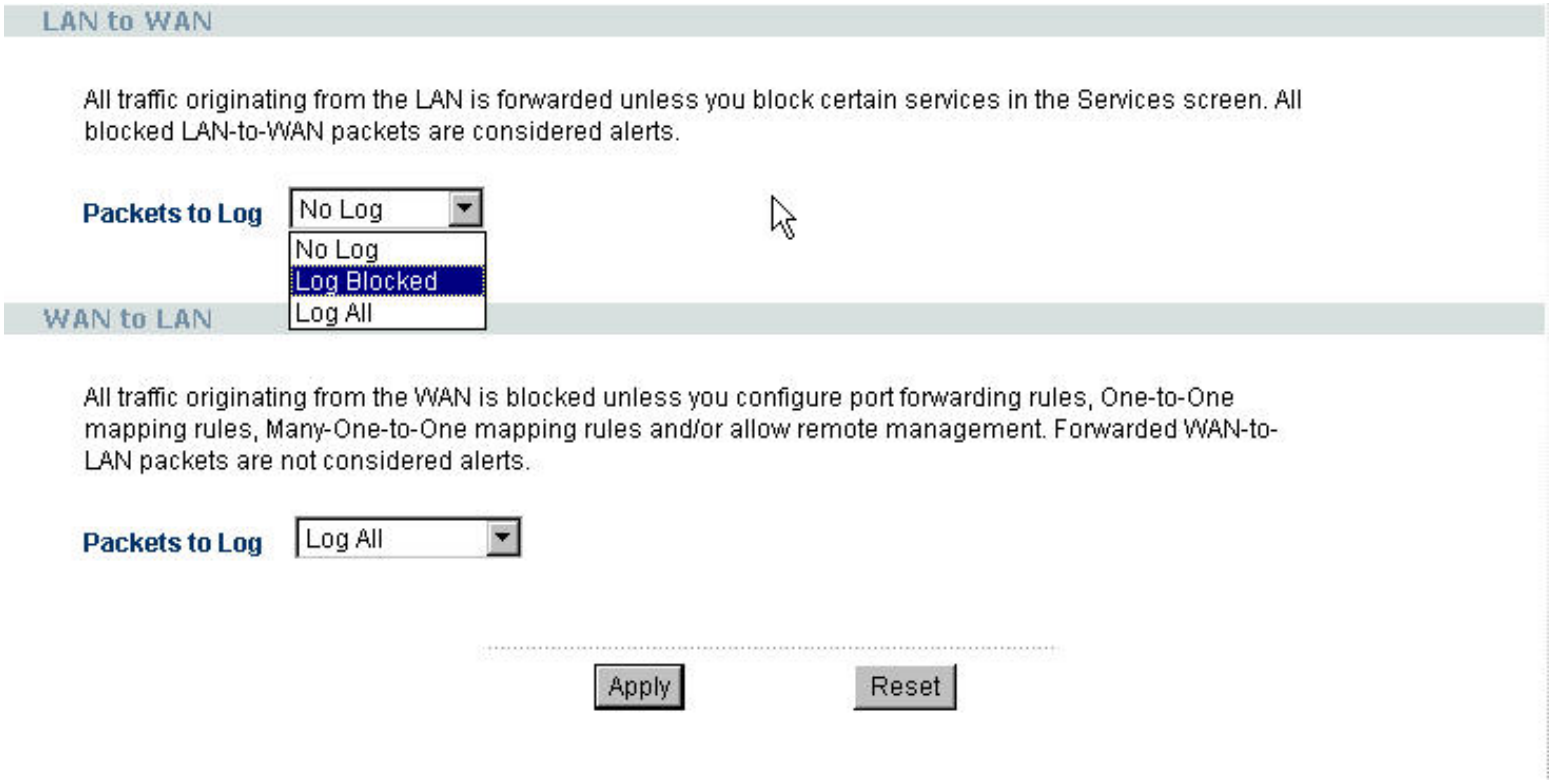
---

1. When does the P334WT generate the firewall log?

The P334WT generates the log immediately when DOS attack is detected.

2. What is contained in P334WT firewall log ?

By default, P334WT pre-configures 4 ACLs, 1)LAN-to-WAN (SET1) 2)WAN-to-LAN (SET2) 3) LAN-to-LAN/P324 (SET7) 4) WAN-to-WAN/P324(SET8). Default policy of set 1 is "forward" and default policy of set 2 is "block". There are four types including No Log, Log Forward, Log Block and Log All options which users can choose which packets to log via WEB Configurator. Both set 7 & 8 are invisible to the users. Default policy of set 7 is "forward" and default policy of set 8 is "block". The log mechanism of set 8 will follow the same configuration as that of set 2.



3. How do I view the firewall log?

The log keeps 128 entries, the new entries will overwrite the old entries when the log has over 128 entries. The firewall log can be viewed via Web Configurator.

All logs generated in P334WT, including firewall logs and system logs are migrated to centralized logs. So you can view firewall logs in Centralized logs.

Before you can view firewall logs there are two steps you need to do,

1. Enable log function in Centralized logs setup via either one of the following methods,

- Web configuration: **Advanced/Logs/Log Settings**, check **Access Control** and **Attacks** options depending on your real situation.
- CI command: **sys logs category [access | attack]**

2. Enable log function in firewall default policy or in firewall rules.

After the above two steps, you can view firewall logs via

1. Web Configurator: **Advanced/Logs**
2. View the log by CI command: **sys logs disp**

You can also view Centralized logs via **mail** or **syslog**, please configure mail server or Unix Syslog server in **Advanced/Logs/ Log Settings**.

4. When does the Prestige generate the firewall alert?

The Prestige generates the alert when an attack is detected by the firewall and sends it via Email. So, to send the alert you must configure the mail server and Email address using Web Configurator. You can also specify how frequently you want to receive the alert via Web Configurator.

5. What does the alert show to us?

The alert shown in the Email is actually the evens of the attack. So, the ***Reason*** column shows ***Attack*** and the ***attack type***. Please see the example shown below.

```
#  Time      Packet Information                Reason   Action

127|Mar 15 0 |From:192.168.1.1 To:192.168.1.1  |attack  |block
   | 03:04:54|ICMP    type:00008    code:00000 |land    |
```

6. What is the difference between the log and alert?

A log entry is just added to the log inside the P334WT and e-mailed together with all other log entries at the scheduled time as configured. An alert is e-mailed immediately after an attacked is detected.

Content Filter FAQ

---

1. What types of content filter does P334WT provide?

P334WT supports three types of content filterings.

- Restrict Web Data including ActiveX, Java Applet, Cookie, Web proxy
- URL keywords

2. How many URL keywords does P334WT support?

64 keywords are supported.

3. What kinds of URL checking methods does P334WT support?

Full path URL checking is supported by P334WT. Now it can parse full URL path for blocking, and the URL checking can be case insensitive. To check URL by domain and directory, users can use a CI commands “ip urlfilter customize actionFlags act5 enable / disable” in menu 24.8. To check domain, directory and filename (*.htm), users have to use another CI command “ip urlfilter customize actionFlags act6 enable/ disable”.

IPSec FAQ

VPN Overview

P334WT VPN

---

1. 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.

2. 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.

3. 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).

4. 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.

5. 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.

6. 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.

7. 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).

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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 P334WT 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.

14. What is FQDN?

FQDN(Fully Qualified Domain Name), IKE standard takes it as one type of Phase 1 ID.

As we mentioned, Phase 1 ID is an identification for each VPN peer. The type of Phase 1 ID may be IP/FQDN(DNS)/Ueser 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 P334WT, if "DNS" or "E-mail" type is chosen, you can still use a random string as the content, such as "this_is_P334WT". It's not necessary to follow the format exactly.

By default, P334WT takes IP as phase 1 ID type for itself and it's remote peer. But if it's remote peer is using DNS or E-mail, you have to adjust the settings to pass phase 1 ID checking.

15. When should I use FQDN?

If your VPN connection is P334WT to P334WT/ZyWALL, 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 .

---

1. Does my P334WT support IPSec VPN?

IPSec VPN is available for P334WT since ZyNOS V3.60.

2. How do I configure P334WT VPN?

You can configure P334WT for VPN using SMT or Web configurator.

3. How many VPN connections does P334WT support ?

P334WT supports 2 tunnels.

4. What VPN protocols are supported by P334WT ?

P334WT supports ESP (protocol number 50) and AH (protocol number 51).

5. What types of encryption does P334WT VPN support?

P334WT supports 56-bit DES and 168-bit 3DES.

6. What types of authentication does P334WT VPN support?

VPN vendors support a number of different authentication methods. P334WT 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.

7. I am planning my P334WT-to-ZyWALL VPN configuration. What do I need to know?

First of all, P334WT is designed for Telecommutor and it works as a client side of the VPN.

If your P334WT and ZyWALL support 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 P334WT, please make sure the NAT router supports to pass through IPSec.
2. In NAT case (either run on the frond end router, or in P334WT VPN box), only IPSec ESP tunneling mode is supported since NAT against AH mode.
3. **Source IP/Destination IP**-- P334WT only supports SINGLE for Local Addr Type in its VPN rules. Therefore, only one PC assigned in the Local IP Addr of VPN rule can be protected via VPN/IPSec. Remote IP Addr can be a Subnet, Range or single host.
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 P334WT for making VPN connections. If it is a dynamic IP given by ISP, you still can configure this IP address after the remote P334WT/ ZyWALL is on-line and its WAN IP is available from ISP.

8. Does P334WT VPN support NetBIOS broadcast?

Yes, P334WT supports NetBIOS broadcast over IPSec VPN tunnel. Use CI command “ipsec config netbios active <yes|no>” in SMT menu 24.8 to enable/disable this function.

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

If P334WT stays in menu 24.1 and 24.8 a certain of memory is allocated to generate the required statistics. So, we do not suggest to stay in menu 24.1 and 24.8 when VPN is in use.

10. How do I configure P334WT with NAT for internal servers?

Generally, without IPSec, to configure an internal server for outside access, we need to configure the server private IP and its service port in SUA/NAT Server Table.

However, if both NAT and IPSec is enabled in P334WT, the edit of the table is necessary only if the connection is a non-secure connections. For secure connections, none SUA server settings are required since private IP is reachable in the VPN case.

For example:

host----P334WT(NAT)----ADSL Modem----Internet----Secure host
\
\
Non-secure host

11. I am planning my P334WT behind a NAT router. What do I need to know?

Some tips for this:

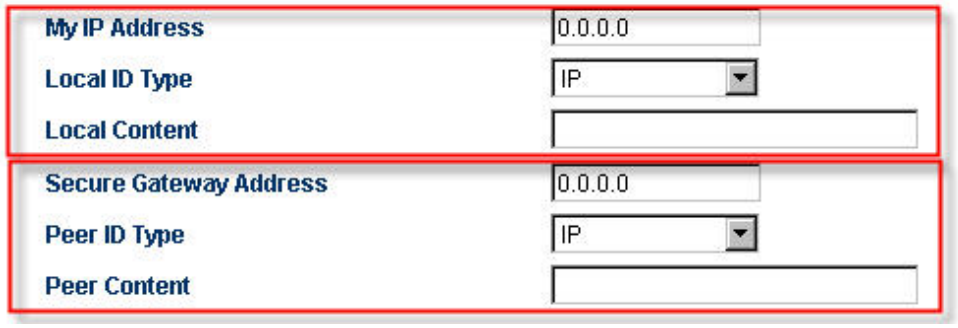
1. The NAT router must support to pass through IPSec protocol. Only ESP tunnel mode is possible to work in NAT case. In the NAT router is P334WT NAT router supporting IPSec pass through, default port and the P334WT WAN IP must be configured in SUA/ NAT Server Table.
2. WAN IP of the NAT router is the tunneling endpoint for this case, not the WAN IP of P334WT.
3. If firewall is turned on in P334WT, you must forward **IKE** port in Internet interface.
4. If NAT are also enabled in P334WT, NAT server is required for non-secure connections, NAT server is not required for secure connections and the physical private IP is used.

For example:

host----P334WT----NAT Router----Internet----Secure host
\
\
Non-secure host

12. Where can I configure Phase 1 ID in P334WT?

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.



13. How to configure P334WT that supports so that it can cooperate with ZyWALL V3.50 ?

ZyWALL with firmware version V3.50 in prefix can only support phase 1 ID as IP type. And ID checking mechanism is actually bypassed. So to work smoothly, please apply IP type in P334WT. The following is an example for your reference.

In this example, we presume that the network environment is as following,

P334WT (V3.60) is using dynamic IP address, and it have DDNS to register it's current dynamic IP address. ZyWALL (V3.50) is using static IP adderss, and since it's peer's IP address is dynamic, so the secure gateway is configured in DDNS format.

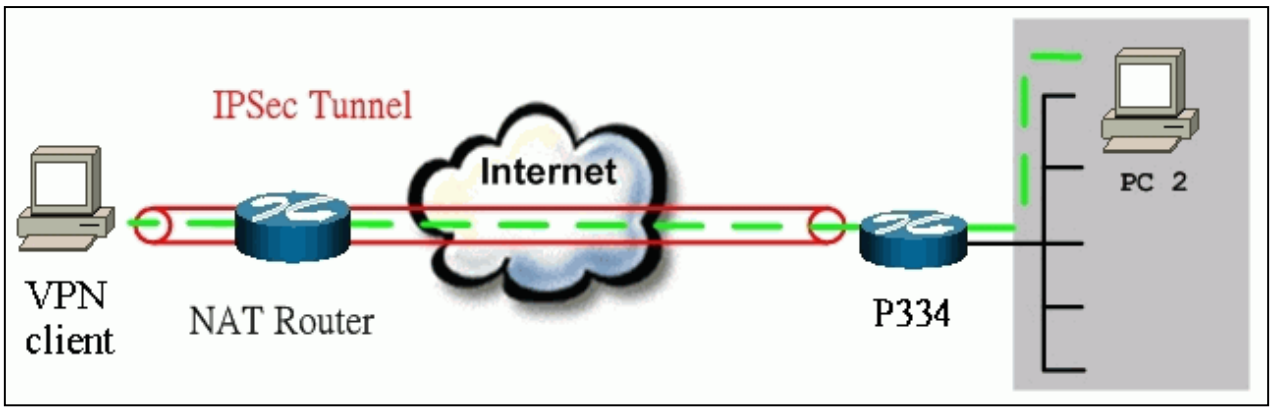
Old ZyWALL (V3.50)	P334WT (V3.60)

My IP=212.125.177.2 Secure gateway Addr= P334WT.dyndns.org (DDNS name of P334WT)	Local ID type = IP My IP = 0.0.0.0 Peer ID type = IP Secure gateway Addr= 212.125.177.2

Old ZyWALL will use the "P334WT.dyndns.org" to find the P334WT's current WAN IP address. And then use it for phase 1 ID content.

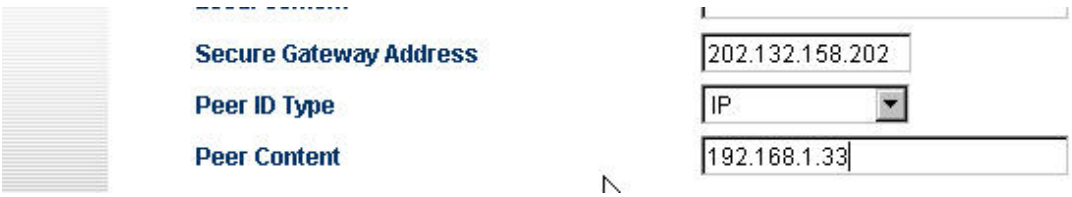
14. If I have NAT router between two VPN gateways, and I would like to use IP type as Phase 1 ID, what should I know?

We presume your environment may look like this,



VPN client: 10.1.33.33
NAT router WAN IP: 202.132.154.2
P334WT 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 P334WT's secure gateway's phase 1 ID as the private IP address of the VPN client. The configuration will be like this,



15. 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.

16. Can the whole LAN behind P334WT be protected by VPN/IPSec tunnel?

No, it can't. P334WT is designed for Telecommuter. Only one PC assigned in the Local IP Addr of VPN rule can be protected via VPN/ IPSec.

17. Can P334WT support IPSec passthrough?

Yes, P334WT can support IPSec passthrough. P334WT doesn'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 P334WT, no configuration is necessary for NAT nor Firewall.

If the VPN connection is initiated from the security gateway outside of P334WT, 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).

18. Can P334WT behave as a NAT router supporting IPSec passthrough and an IPSec gateway simultaneously ?

No, current P334WT can't support them simultaneously. You need to choose either one. If P334WT is to support IPSec passthrough, you have to disable the VPN function on P334WT. 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. P334WT may support both of them in the future, please refer to the release note.

Wireless FAQ

General FAQ

Advanced FAQ

Security FAQ

Basic FAQ

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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).

9. 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.

10. 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 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.

11. 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.

12. 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.

13. 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.

14. 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 same2.4-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 interefere. 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.

15. 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.

16. 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.

17. 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.

Advanced FAQ

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

Security FAQ

1. How do I secure the data across an Access Point's radio link ?

Enable Wired Equivalency Protocol (WEP) to encrypt the payload of packets sent across a radio link.

2. 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.

3. 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.

4. What is a WEP key ?

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

5. Will 128-bit WEP communicate with 64-bit WEP ?

No. 128-bit WEP will not communicate with 64-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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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*.

12. What is the difference between force-authorized, force-unauthorized and auto ?

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.

force-unauthorized—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.

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. 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.

13. 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.

14. 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.

Prestige 334WT 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.

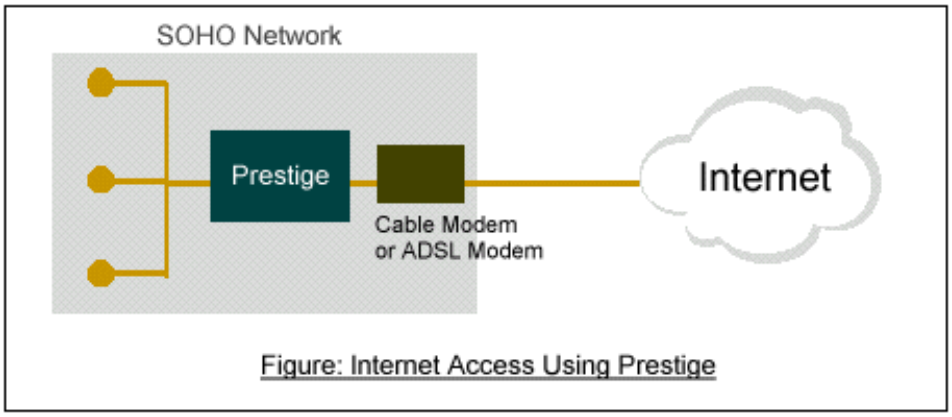


Figure: Internet Access Using Prestige

- **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 Windows**

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.

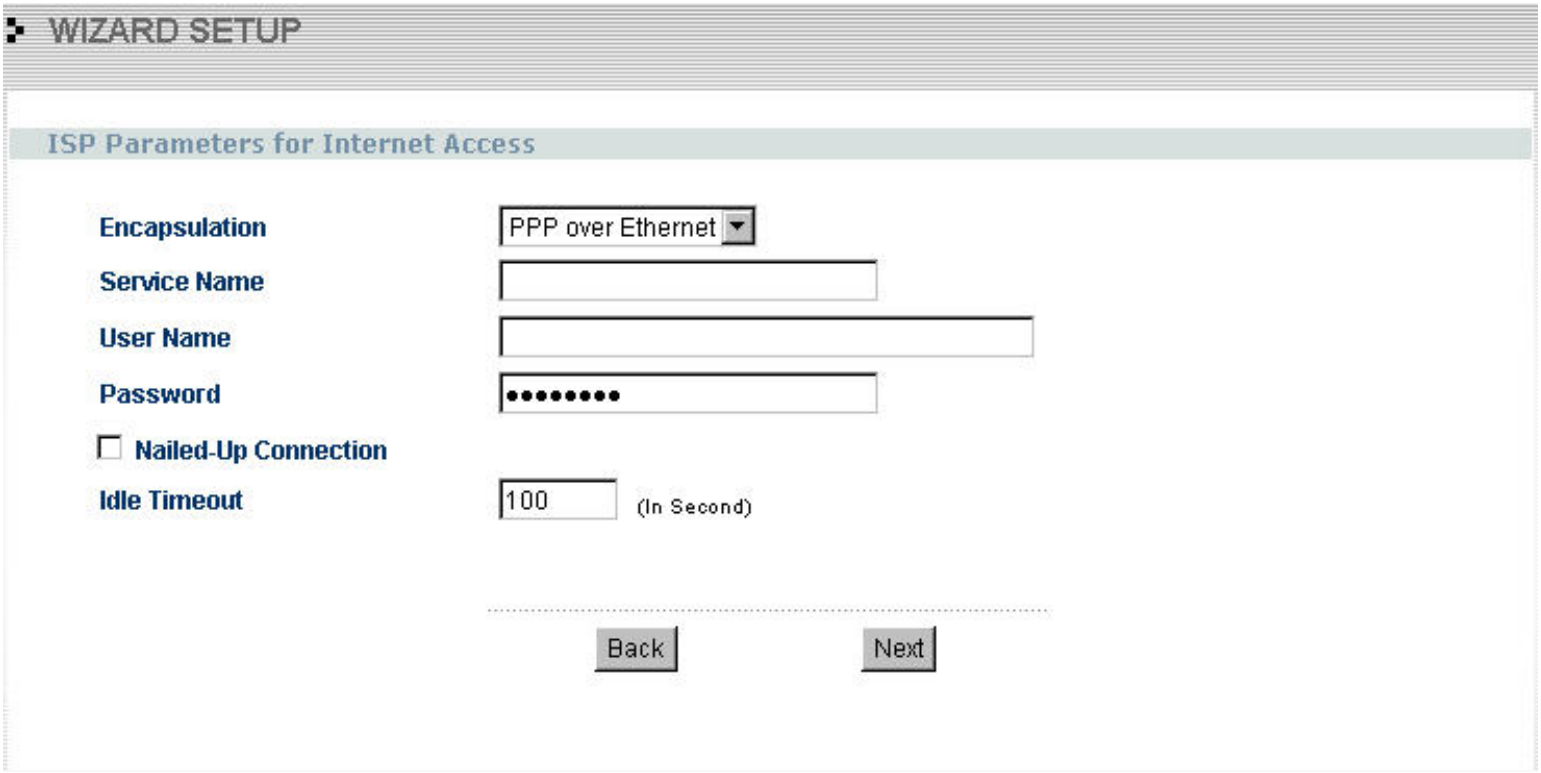
1. Retrieve Prestige Web

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.

2. Login first

To restrict only the adminstrator can configure the router, there is a login procedure prompted for asking User Name and Password. The default User Name is '**admin**' and 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.

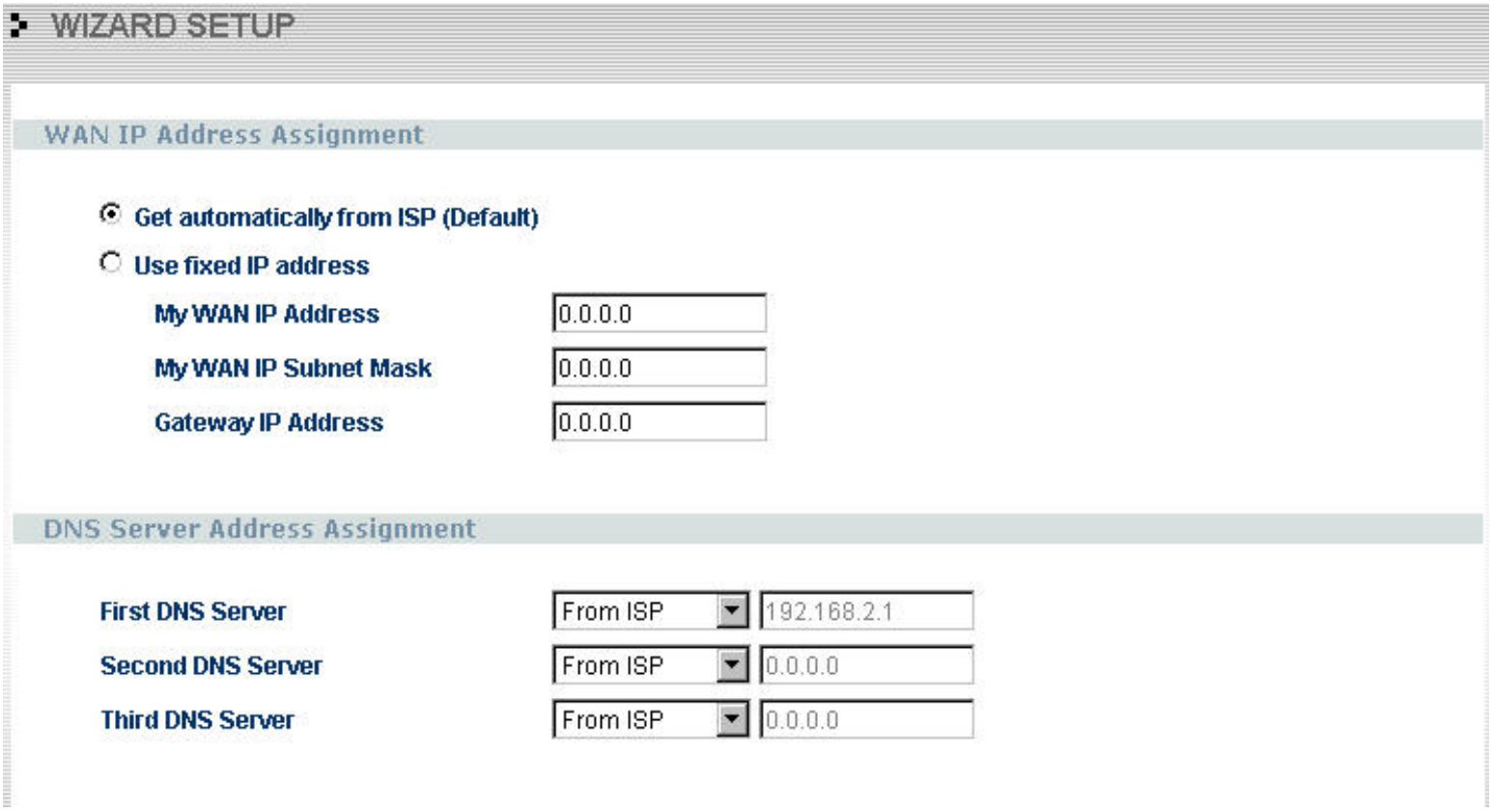


Key Settings:

Option	Description
Encapsulation	Select the encapsulation type your ISP supports
Service Name	Enter the **'Service Name'** for the ISP
User Name	Enter the login user name given by the ISP
Password	Enter the password given by the ISP
Idle Timeout	This value specifies the time in seconds that can elapse before the Prestige automatically disconnects the PPPoE connection.

4. WAN IP Address Assignment

Check **'Get automatically from ISP'** if the ISP provides the IP dynamically, otherwise check **'Use fixed IP address'** and enter the static IP in the **'IP Address'** field.



5. Check if the connection is up by clicking the ADVANCED/MAINTENANCE menu.

Setup the Prestige for PPPoE Connections

- Introduction

PPP over Ethernet is an IETF draft standard specifying how a host personal computer (PC) 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 several major service providers running evaluations of PPPoE today. Before using PPPoE feature of the Prestige, please make sure your ISP supports PPPoE.

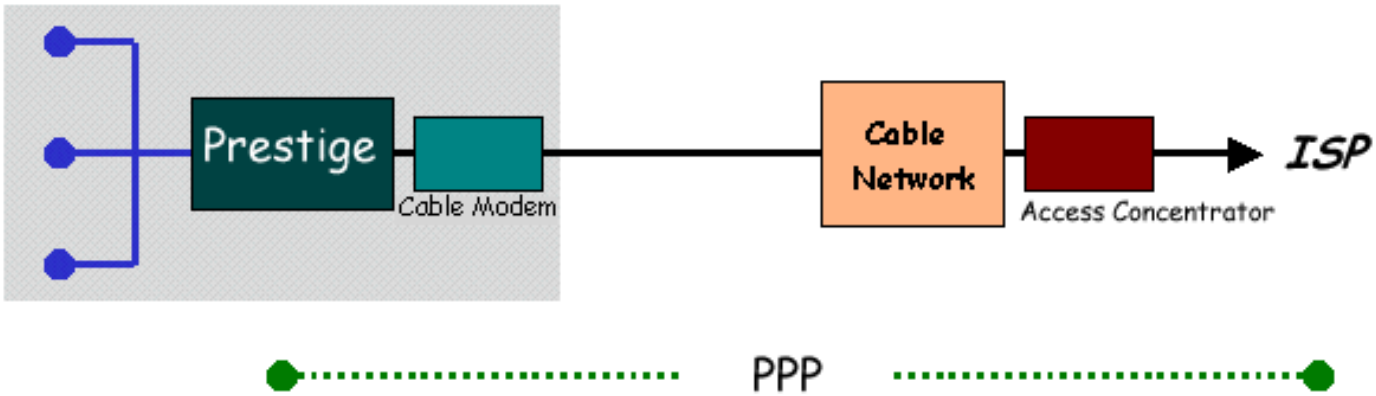


Figure1: Prestige as a PPPoE Client

- Setup the Prestige for Internet Access using PPPoE

1. Configure Encapsulation/IP Address Assignment/NAT in SMT Menu 4

```
                Menu 4 - Internet Access Setup

                  ISP's Name= ChangeMe
                  Encapsulation= PPPoE
                  Service Type= N/A
                    My Login= ras@pppoellc
                    My Password= ********
                    Idle Timeout= 100

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


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

Key Settings for making a PPPoE connection:

Option	Description
Encapsulation	Set '**PPPoE**' as the encapsulation.
My Login	Enter the login name that the ISP provided.
My Password	Enter the password that the ISP provided.
Idle Timeout	This value specifies the time in seconds that can elapse before the Prestige automatically disconnects the PPPoE connection.
IP Address Assignment	Choose '**Dynamic**' if the ISP provides the IP dynamically, otherwise choose '**Static**' and enter the static IP in the '**IP Address**' field.
Network Address Translation	Set this field to '**SUA Only**' if you want all clients share one IP to Internet. Set to '**Full Feature**' if there are multiple IP addresses given by ISP and can assigned to your clients. Set to '**None**' if you clients use Internet IP addresses and thus do not need NAT function.

2. Configure '**Server Name**' for the PPPoE connection in Menu 11.1

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP
Active= Yes
Apply Alias= None
Encapsulation= PPPoE
Service Type= Standard
Service Name=
Outgoing:
My Login= test
My Password= ********
Retype to Confirm= ********
Authen= CHAP/PAP

Route= IP

Edit IP= No
Telco Option:
Allocated Budget(min)= 0
Period(hr)= 0
Schedules=
Nailed-Up Connection= No

Session Options:
Edit Filter Sets= No
Idle Timeout(sec)= 100

Edit Traffic Redirect= No

Setup the Prestige 334WT as a PPTP Client

- What is PPTP Client?

Microsoft's Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP network. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the Internet.

This implementation of PPTP client is specifically for the French market where Alcatel's ANT (ADSL Network Termination) is deployed. Most, if not all, broadband modems (ADSL and cable modem) are equipped with Ethernet instead of RS-232 because RS-232 is too slow. It is therefore impossible to use them in the same way as the traditional analog modem and ISDN TA. A mechanism is needed to transport the PPP frames from a PC to the broadband modem over Ethernet. Before PPPoE was formalized, Alcatel came up with the idea of building PPTP into their ANT for this purpose.

Instead of using the Internet to transport PPP frames anywhere in the world as originally envisioned, Alcatel's solution uses PPTP only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP.

The various connections in this setup are depicted in the following diagram.

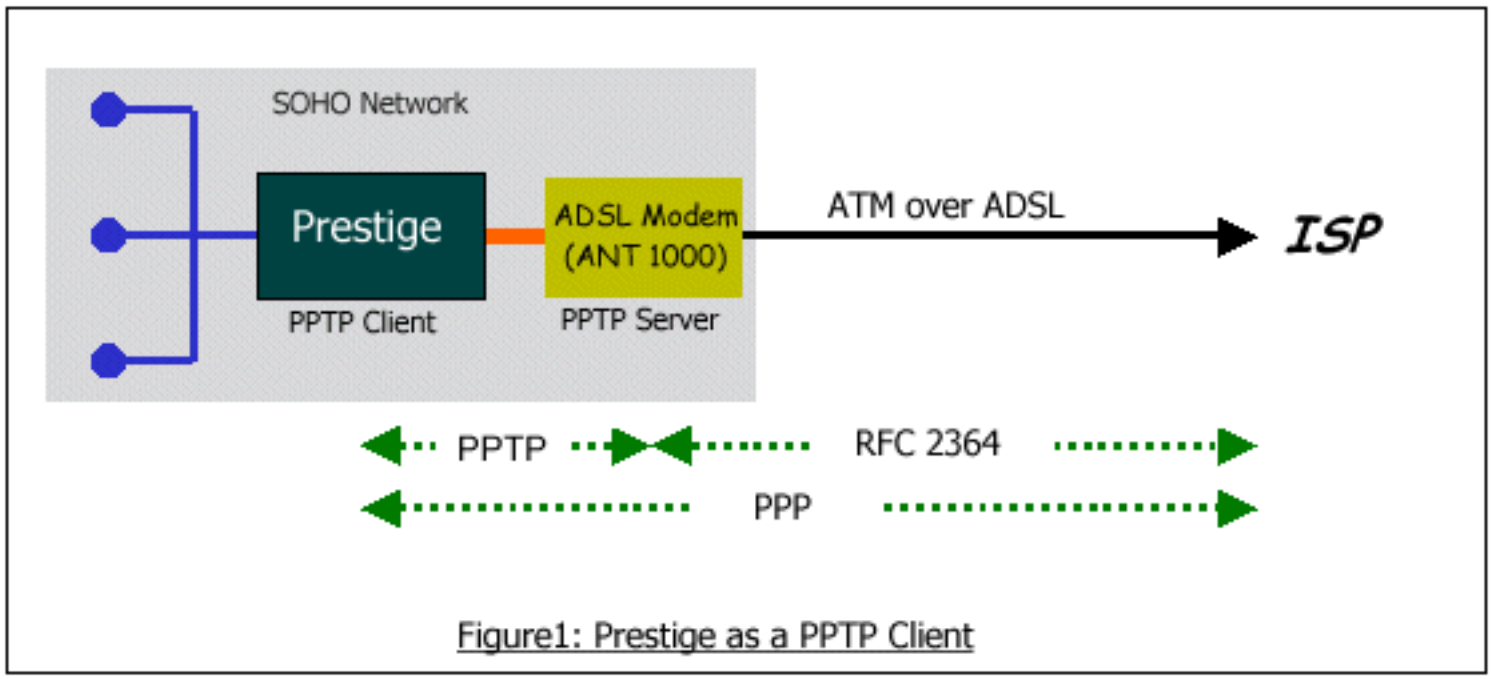


Figure1: Prestige as a PPTP Client

The PPTP client feature means the PPTP connection is initialized by the Prestige 334WT router, so this connection is transparent to the PPTP clients on the network. This eliminates the settings of every

clients and does not matter whether the computers on the network are Windows, Macintosh or even UNIX, all that is required is a standard TCP/IP protocol stack. In fact,
users are unaware that they are on a VPN, since the Prestige 324 does all the VPN work.

- Setup the Prestige 324 as a PPTP client

```
                Menu 4 - Internet Access Setup

                ISP's Name= ChangeMe
                Encapsulation= PPTP
                  Service Type= N/A
                  My Login=
                  My Password= ********
                  Idle Timeout= 100

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

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

Key Settings:

Option	Description
Encapsulation	Set '**PPTP**' as the encapsulation.
My Login	Enter the login name to login the PPTP server.
My Password	Enter the password associated with the login name above.
IP Address Assignment	Choose '**Dynamic**' if the PPTP server provides the IP dynamically, otherwise choose '**Static**'.

IP Address	Enter the IP address supplied by the PPTP server if it provides the IP stactically.
Network Address Translation	Set this field to **'Yes'** to enable the Single User Account feature for your Prestige 324. Use the space bar to toggle between **'Yes'** and **'No'**.

Using Multi-NAT

- What is Multi-NAT?

NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the P334WT, thus preventing intruders from probing your network.

The SUA feature that the P334WT supports previously operates by mapping the private IP addresses to a global IP address. It is only one subset of the NAT. The P334WT 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 P334WT router). The P334WT keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

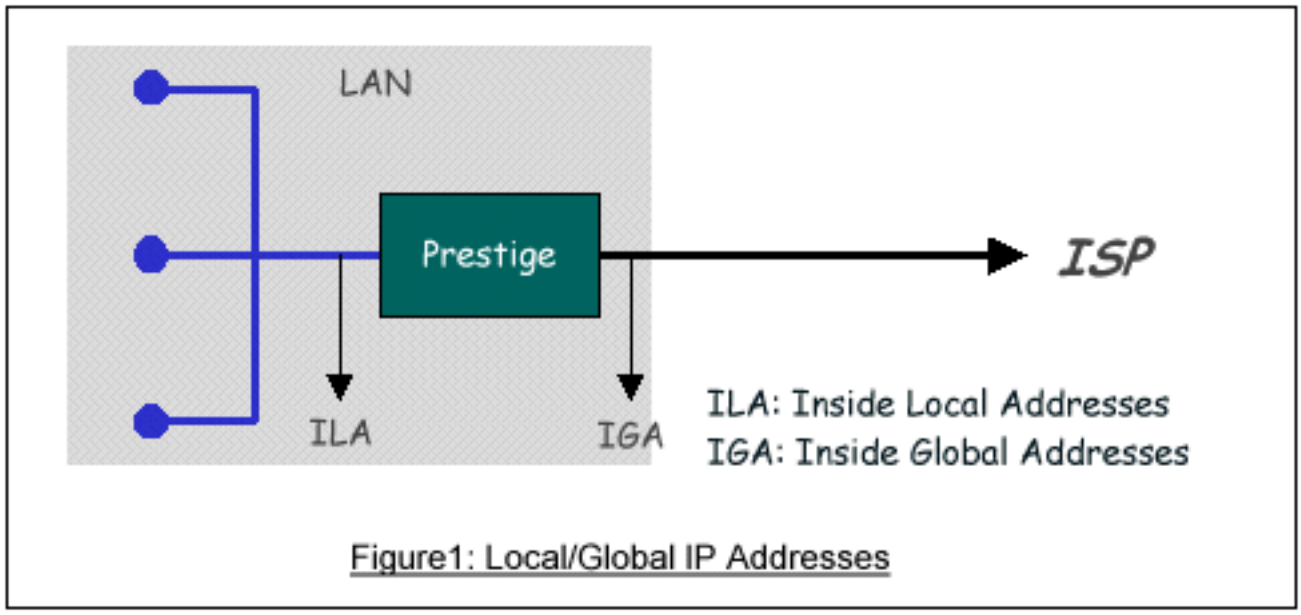


Figure1: Local/Global IP Addresses

- NAT Mapping Types

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

1. **One to One**

   In One-to-One mode, the P334WT maps one ILA to one IGA.

2. **Many to One**

   In Many-to-One mode, the P334WT 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 P334WT maps the multiple ILA to shared IGA.

4. **Many to Many No Overload**

   In Many-to-Many No Overload mode, the P334WT maps each ILA to unique IGA.

5. **Server**

   In Server mode, the P334WT 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

- SUA Versus NAT

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. The P334WT now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple severs of the same type (e.

g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions (that supported SUA 'visible' servers had to be of different types. The P334WT supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The P334WT 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.

- SMT Menus

1. Applying NAT in the SMT Menus
2. Configuring NAT
3. Address Mapping Sets and NAT Server Sets

---

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= ChangeMe
                Encapsulation= Ethernet
                Service Type= Standard
                  My Login= N/A
                  My Password= N/A
                  Login Server IP= N/A

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



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

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

```
                Menu 11.3 - Remote Node Network Layer Options

                  IP Address Assignment= Dynamic
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  Gateway IP Addr= N/A

                  Network Address Translation= SUA Only
                  Metric= N/A
                  Private= N/A
                  RIP Direction= Both
                    Version= RIP-1


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

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

The following table describes the options for Network Address Translation.

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

Table: Applying NAT in Menu 4 and Menu 11.3

2. Configuring NAT

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

```
                        Menu 15 - NAT Setup

                    1. Address Mapping Sets
                    2. Port Forwarding Setup
                    3. Trigger Port Setup
```

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 P334WT has one remote node and so allows you to configure only 1 NAT Address Mapping Set. You can see two NAT Address Mapping sets in Menu 15.1. You can only configure Set 1. Set 255 is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use Set1. When you select **SUA Only**, the SMT will use Set 255. For the P100IH, there are 8 remote nodes and so allows you to configure 8 NAT Address Mapping Sets.

The NAT Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the P334WT), 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. NAT_SET
            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 (Read Only)

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


                          Press ESC or RETURN to Exit:
```

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

Field	Description	Option/Example
Set Name	This is the name of the set you selected in Menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	This is the starting local IP address (ILA).	0.0.0.0 for the Many-to-One type.
Local End IP	This is the starting local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255

Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	N/A
Type	This is the NAT mapping types.	Many-to-One and Server

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

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

```
                Menu 15.1.1 - Address Mapping Rules

  Set Name= NAT_SET

 Idx  Local Start IP   Local End IP     Global Start IP  Global
End IP    Type
 ---  ---------------  ---------------  ---------------
---------------  ------
  1.
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

                  Action= Edit          , Select Rule= 0

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

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

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

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

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

```
                Menu 15.1.1.1 -  - Rule 1

                Type: One-to-One

                Local IP:
                  Start= 0.0.0.0
                  End  = N/A

                Global IP:
                  Start= 0.0.0.0
                  End  = N/A


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

The following table describes the fields in this screen.

Field		Description	Option/Example
Type		Press [SPACEBAR] to toggle through a total of 5 types. These are the mapping types discussed above plus a server type. Some examples follow to clarify these a little more.	One-to-One Many-to-One Many-to-Many Overload Many-to-Many No Overload Server
Local IP	Start	This is the starting local IP address (ILA)	0.0.0.0
	End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for **One-to-One** type.	255.255.255.255
Global IP	Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
	End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** types.	172.16.23.55

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

- NAT Server Sets

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

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

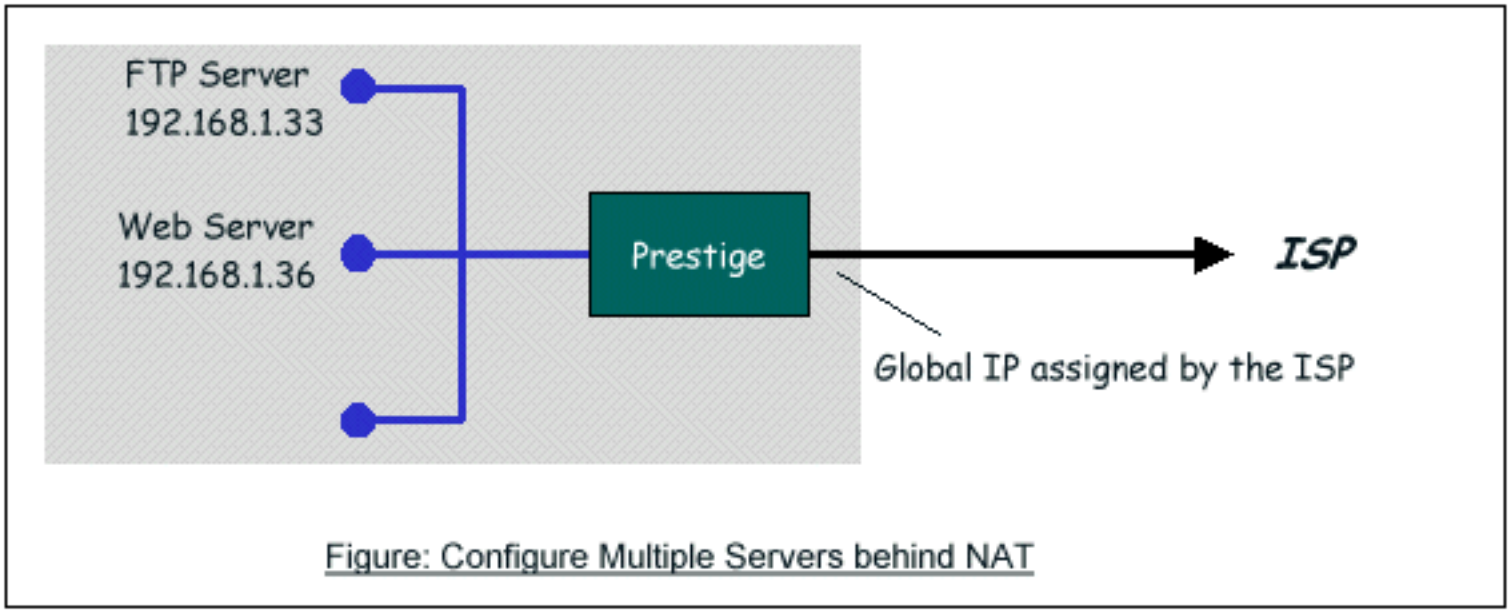


Figure: Configure Multiple Servers behind NAT

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

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

Step 1. Enter 15 in the Main Menu to go to **Menu 15-NAT Setup**.
Step 2. Enter 2 to go to **Menu 15.2-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

Rule Start Port No. End Port No. IP Address
-------------------------------------------------
1.      Default        Default     0.0.0.0
2.        80             80        192.168.1.33
3.        21             21        192.168.1.34
4.        0              0         0.0.0.0
5.        0              0         0.0.0.0
6.        0              0         0.0.0.0
7.        0              0         0.0.0.0
8.        0              0         0.0.0.0
9.        0              0         0.0.0.0
10.       0              0         0.0.0.0
11.       0              0         0.0.0.0
12.       0              0         0.0.0.0
```

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

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

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

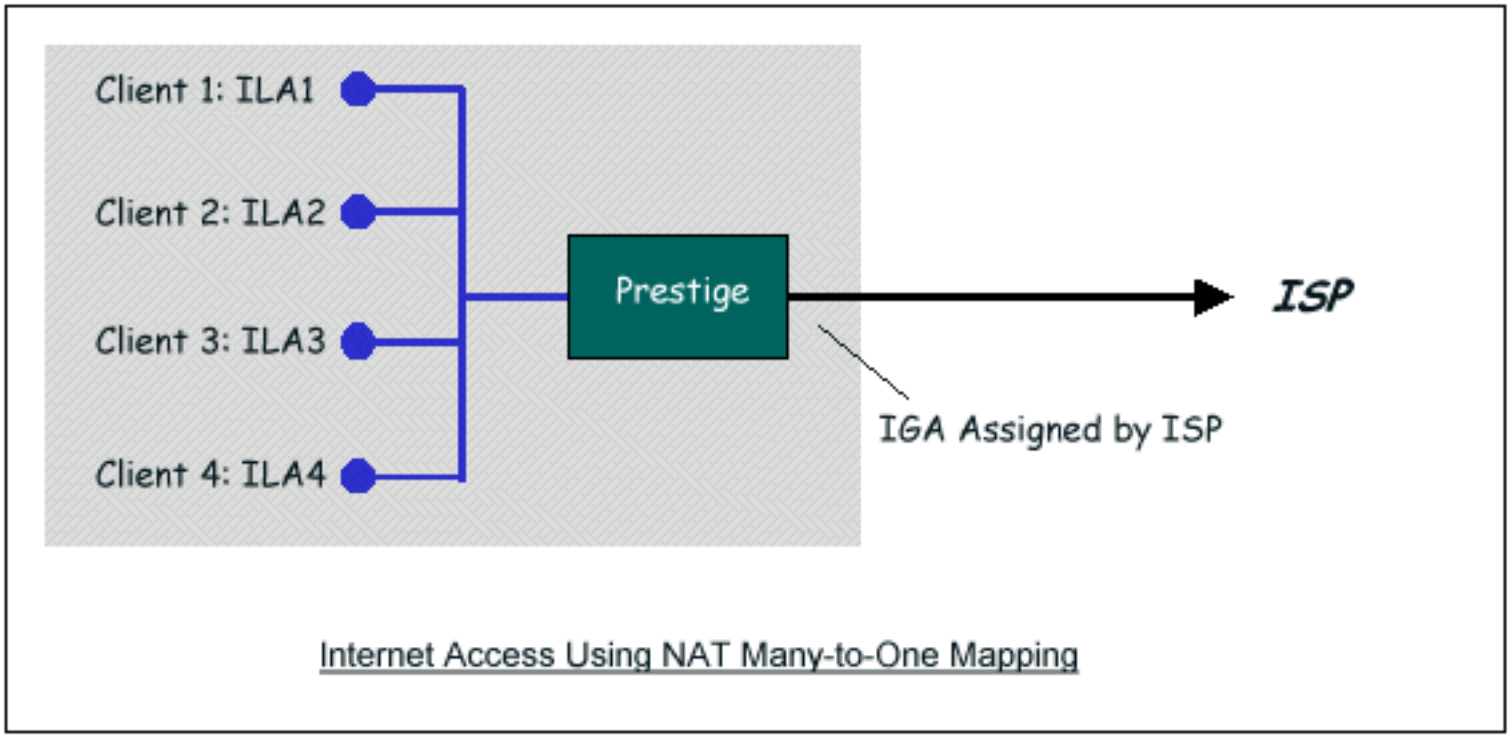
- Examples

1. Internet Access Only
2. Internet Access with an Internal Server
3. Using Multiple Global IP addresses for clients and servers
4. Support Non NAT Friendly Applications

---

1. Internet Access Only

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

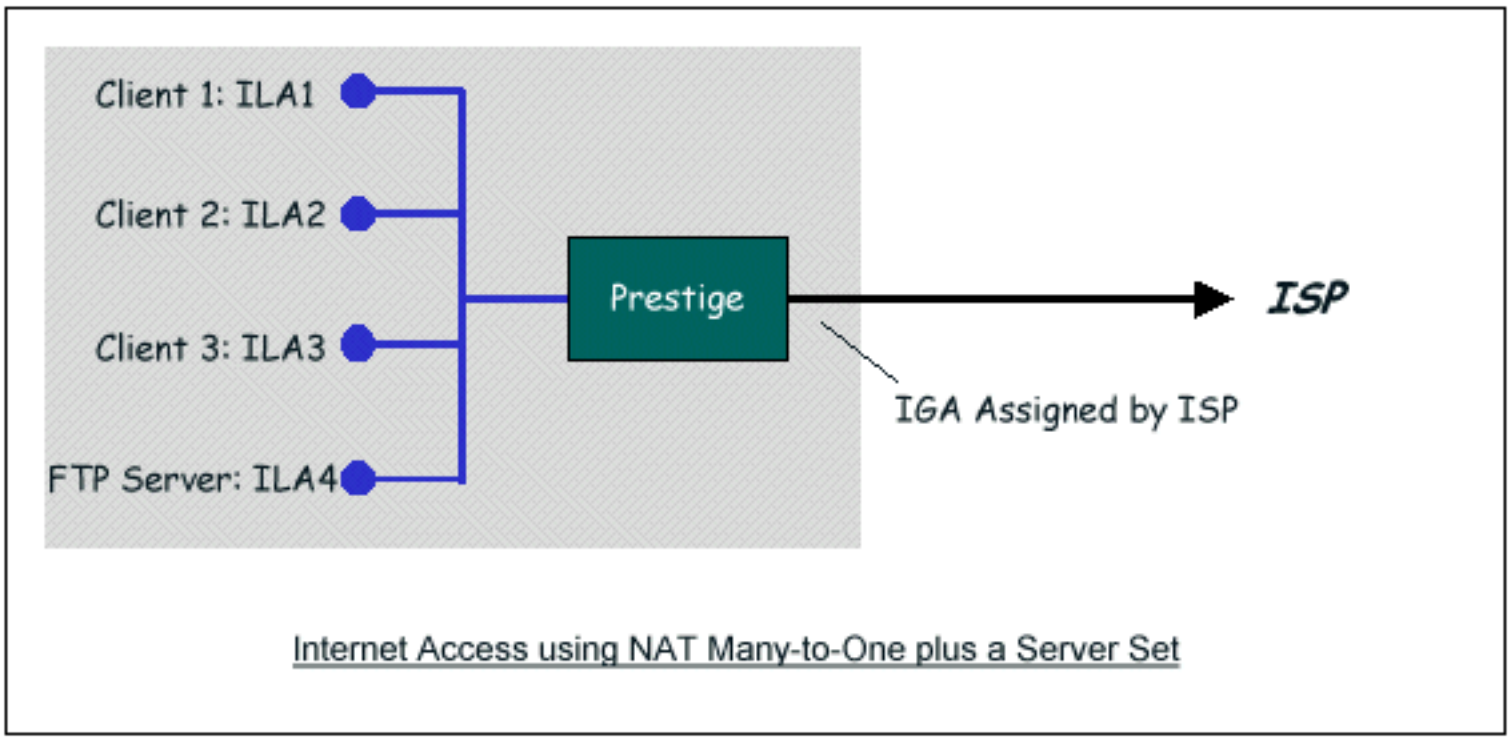


Internet Access Using NAT Many-to-One Mapping

```
                Menu 4 - Internet Access Setup

                 ISP's Name= ChangeMe
                 Encapsulation= Ethernet
                 Service Type= Standard
                   My Login= N/A
                   My Password= N/A
                   Login Server IP= N/A

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



                 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.

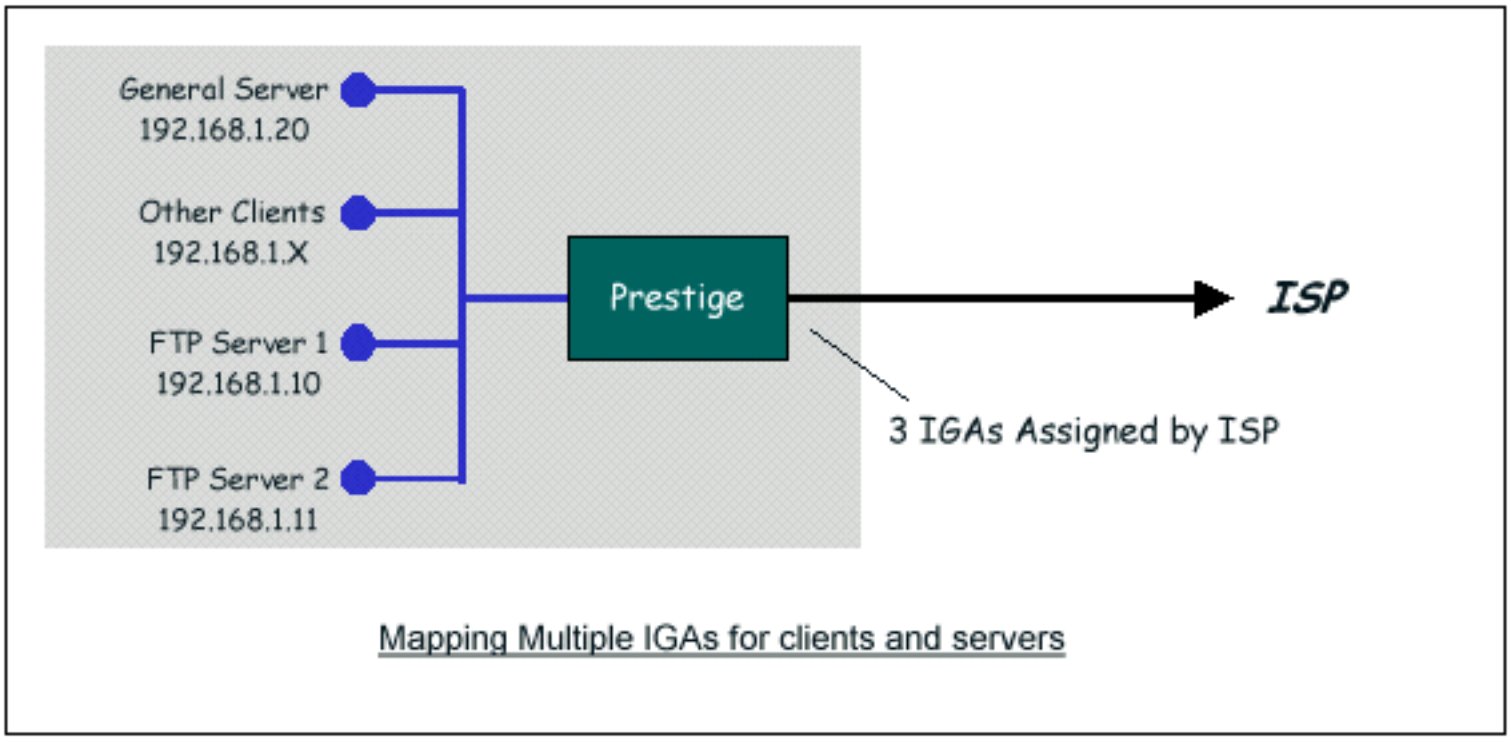
2. Internet Access with an Internal Server



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

```
     Menu 15.2 - NAT Server Setup

Rule Start Port No. End Port No. IP Address
-------------------------------------------------
1.      Default        Default     0.0.0.0
2.        80             80        192.168.1.33
3.        21             21        192.168.1.34
4.        0              0         0.0.0.0
5.        0              0         0.0.0.0
6.        0              0         0.0.0.0
7.        0              0         0.0.0.0
8.        0              0         0.0.0.0
9.        0              0         0.0.0.0
10.       0              0         0.0.0.0
11.       0              0         0.0.0.0
12.       0              0         0.0.0.0

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

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



Mapping Multiple IGAs for clients and servers

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

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

Step 1:

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

```
                Menu 4 - Internet Access Setup

                ISP's Name= ChangeMe
                Encapsulation= Ethernet
                Service Type= Standard
                  My Login= N/A
                  My Password= N/A
                  Login Server IP= N/A

                IP Address Assignment= Dynamic
                  IP Address= N/A
                  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:

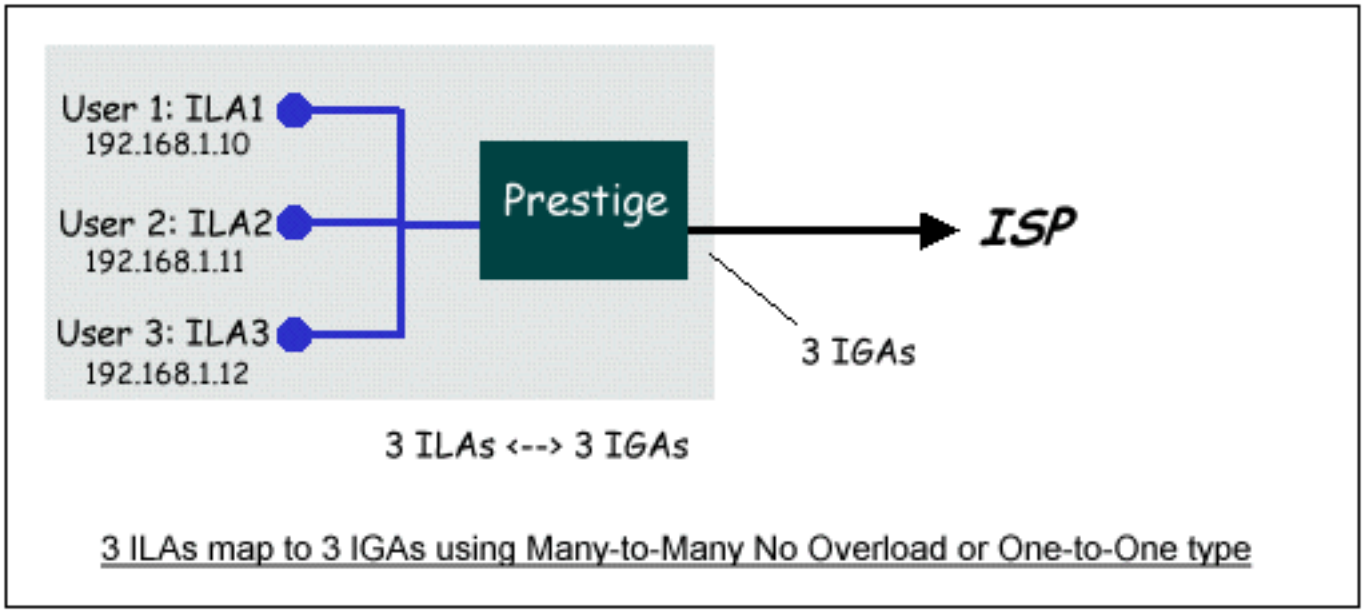
Now we configure all other incoming traffic to go to our web server aand mail server from **Menu 15.2.2 - NAT Server Setup** (not Set 1, Set 1 is used for SUA Only case).

```
                Menu 15.2 - 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.        21           21        192.168.1.11
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:
```

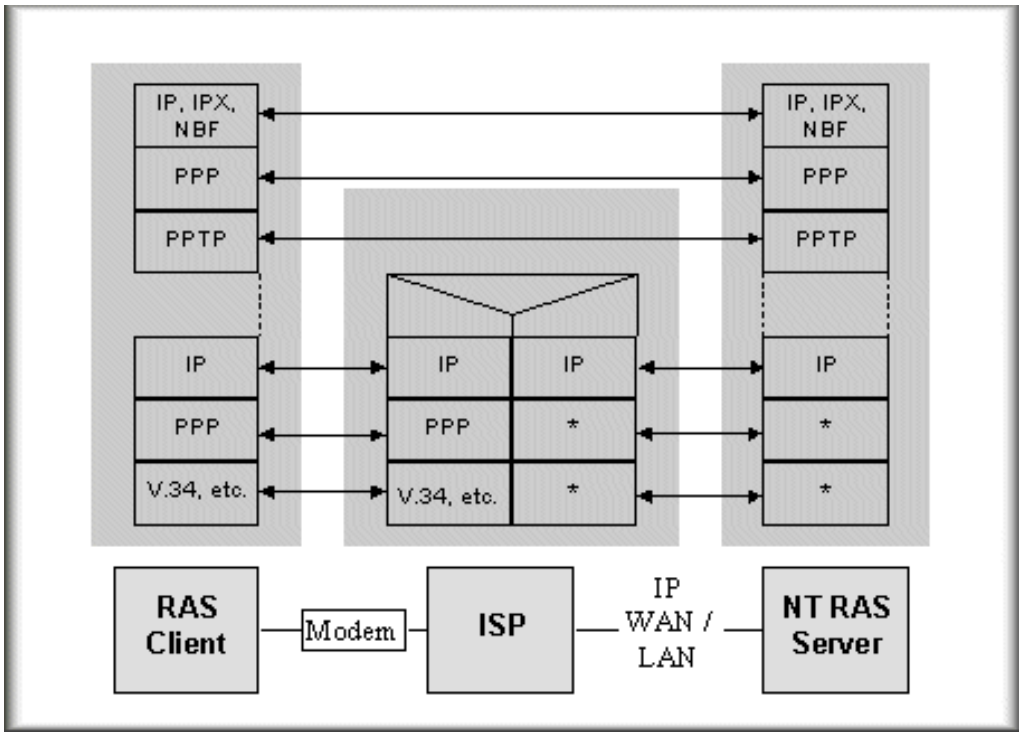
Configure a PPTP server behind SUA

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

Windows Dial-Up Networking uses the Internet standard Point-to-Point (PPP) to provide a secure,optimized multiple-protocol network connection over 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.



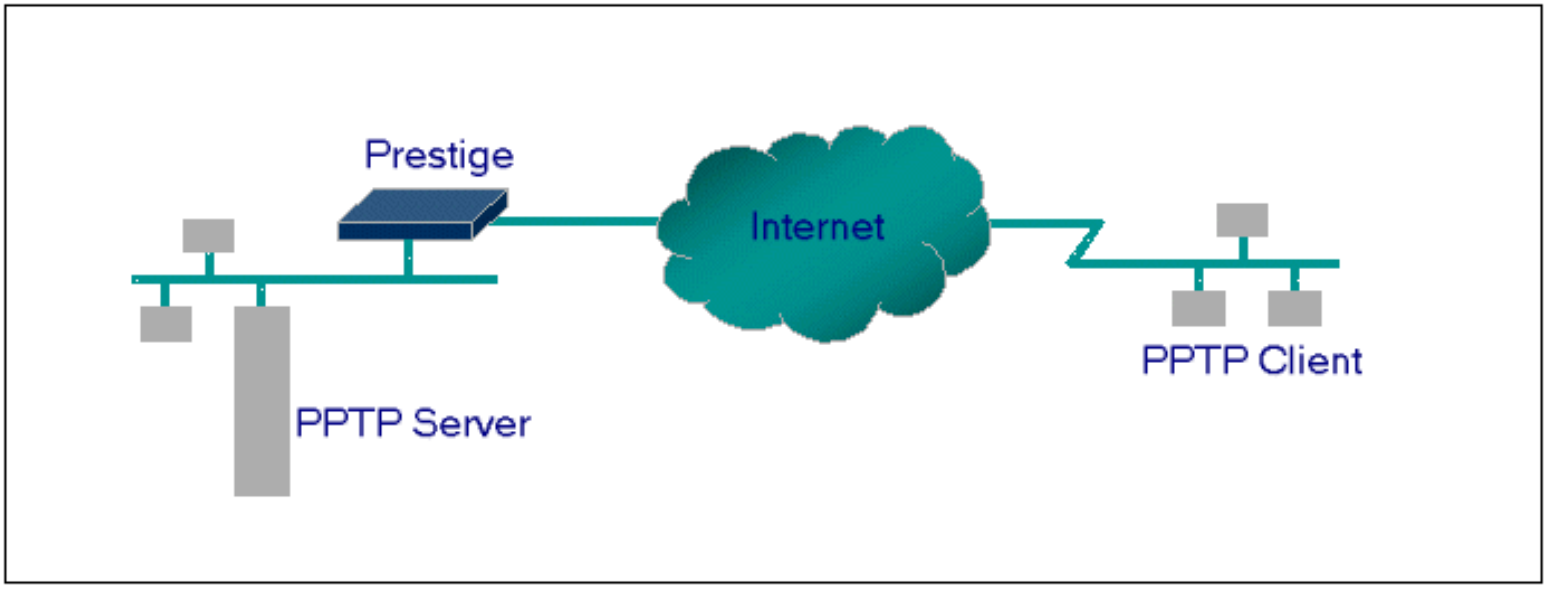
Window95 PPTP Client / Internet / NT RAS Server Protocol Stack

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

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

- Configuration

This application note explains how to establish a PPTP connection with a remote private network in the Prestige 324 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 324 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 334WT 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 324.

  - 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 324
  - 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 324's Internet IP address for logging to NT RAS server.
    - Set the Internet gateway to the router that is connecting to ISP
  - Prestige 334WT router setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect Prestige 334WT 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 - SUA Server Setup


          Port #          IP  Address
          ------        ---------------
        1.Default       0.0.0.0
        2. 1723         192.168.1.10
        3. 0            0.0.0.0
        4. 0            0.0.0.0
        5. 0            0.0.0.0
        6. 0            0.0.0.0
        7. 0            0.0.0.0
        8. 0            0.0.0.0
```

```
                9. 0            0.0.0.0
```

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 achive, you can place a VPN call from the remote Win9x client.

For example:

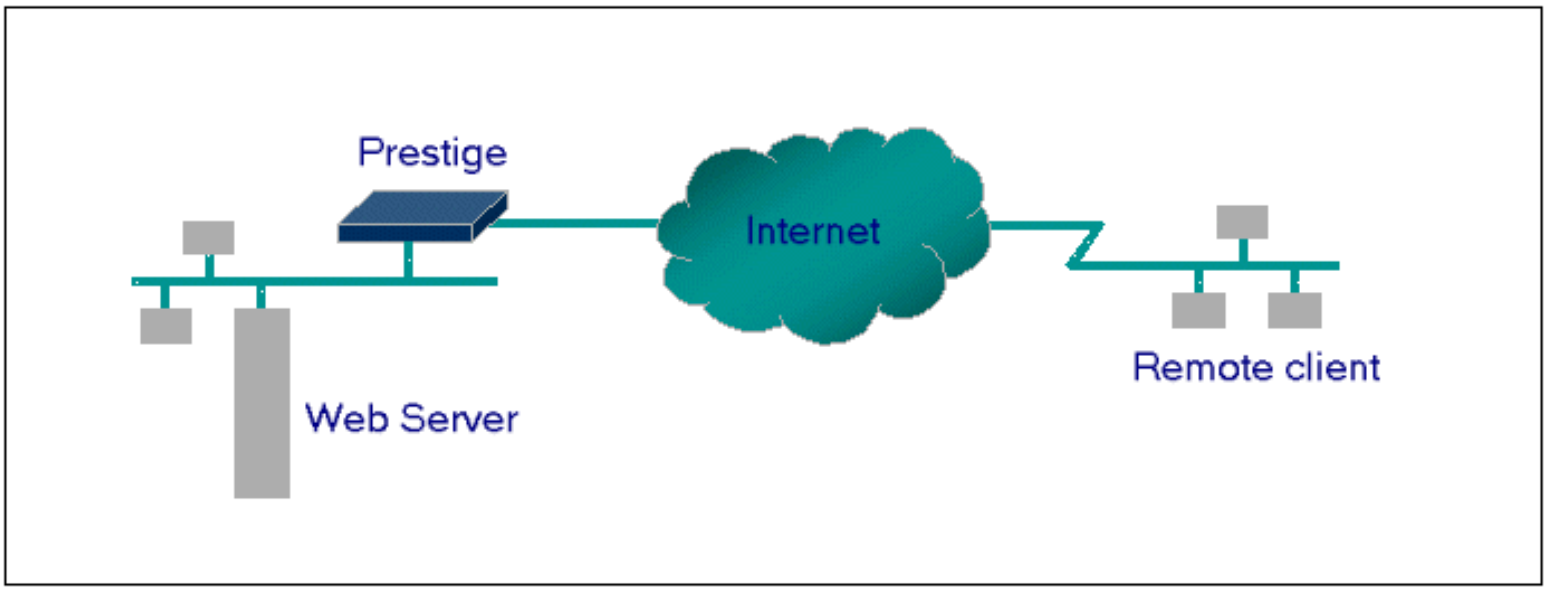
C:\ping 203.66.113.2

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 Win95 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 324 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.

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', Multiple Server Configuration. The outside users can access the local server using the Prestige's ***WAN IP*** address which can be obtained from menu 24.1.

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

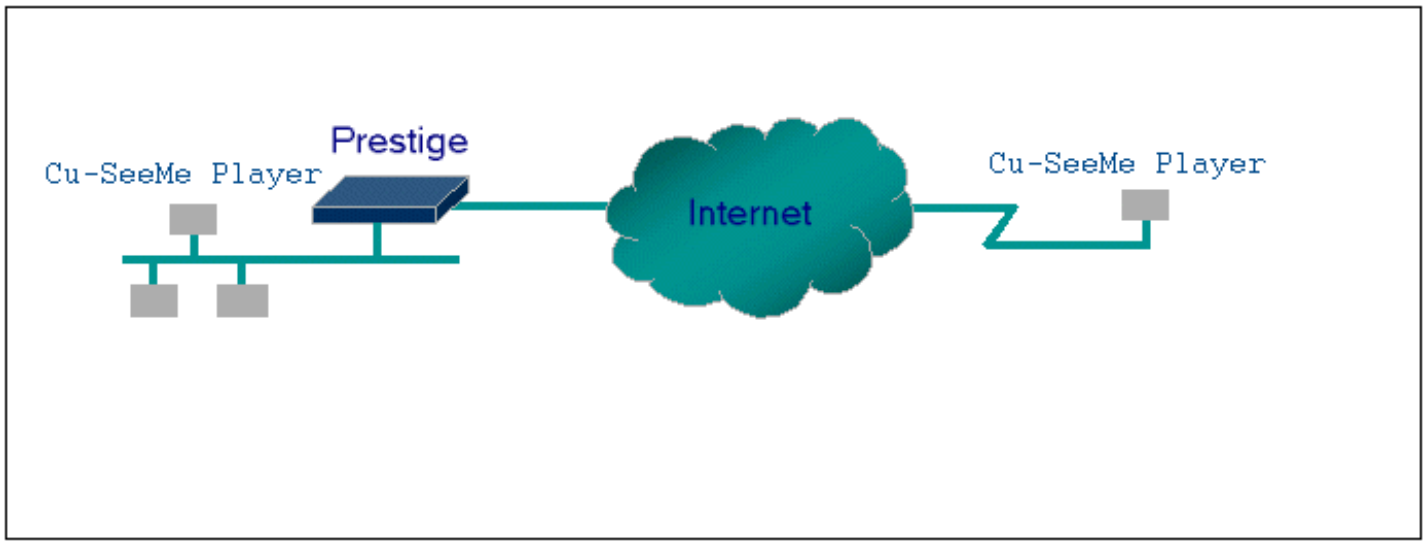
```
                Menu 15 - SUA Server Setup


          Port #            IP  Address
          ------        ---------------
        1.Default       0.0.0.0
        2. 80           192.168.1.10
        3. 0            0.0.0.0
        4. 0            0.0.0.0
        5. 0            0.0.0.0
        6. 0            0.0.0.0
        7. 0            0.0.0.0
```

```
8. 0              0.0.0.0
```

- Port numbers for some services

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

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



- Introduction

Generally, SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. However, some applications such as Cu-SeeMe, and ICQ will need to connect to the local user behind the Prestige. In such case, a **SUA server** must be entered in menu 15 to forward the incoming packets to the true destination behind SUA. Generally, we do not need extra settings of menu 15 for an outgoing connection. But for some applications we need to configure the menu 15 to make the outgoing connection work. After the required menu 15 settings are completed the internal server or client applications can be accessed by using the Prestige's ***WAN IP*** address.

- SUA Supporting Table

The following are the required menu 15 settings for the various applications running SUA mode.

ZyXEL SUA Supporting Table[1]

Application	Required Settings in Menu 15 Port/IP	
	Outgoing Connection	Incoming Connection
HTTP	None	80/client IP
FTP	None	21/client IP
TELNET	None	23/client IP (and remove Telnet filter in WAN port)
POP3	None	110/clinet IP
SMTP	None	25/client IP
mIRC	None for Chat. For DCC, please set Default/Client IP	
Windows PPTP	None	1723/client IP

ICQ 99a	None for Chat. For DCC, please set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
ICQ 2000b	None for Chat	None for Chat
ICQ Phone 2000b	None	6701/client IP
Cornell 1.1 Cu-SeeMe	None	7648/client IP
White Pine 3.1.2 Cu-SeeMe[2]	7648/client IP & 24032/client IP	Default/client IP
White Pine 4.0 Cu-SeeMe	7648/client IP & 24032/client IP	Default/client IP
Microsoft NetMeeting 2.1 & 3.01[3]	None	1720/client IP 1503/client IP
Cisco IP/TV 2.0.0	None	
RealPlayer G2	None	
VDOLive	None	
Quake1.06[4]	None	Default/client IP
QuakeII2.30[5]	None	Default/client IP
QuakeIII1.05 beta	None	
StartCraft	6112/client IP	
Quick Time 4.0	None	
pcAnywhere 8.0	None	5631/client IP 5632/client IP 22/client IP
IPsec (ESP tunneling mode, NAT-T tunnel/transport)	None (one client only)	Default/Client
Microsoft Messenger Service 3.0	6901/client IP	6901/client IP
Microsoft Messenger Service 4.6/ 4.7/ 5.0 (none UPnP)[6]	None for Chat, File transfer ,Video and Voice	None for Chat, File transfer, Video and Voice
Net2Phone	None	6701/client IP
Network Time Protocol (NTP)	None	123 /server IP
Win2k Terminal Server	None	3389/server IP
Remote Anything	None	3996 - 4000/client IP
Virtual Network Computing (VNC)	None	5500/client IP 5800/client IP 5900/client IP
AIM (AOL Instant Messenger)	None for Chat and IM	None for Chat and IM
e-Donkey	None	4661 - 4662/client IP
POLYCOM Video Conferencing	None	Default/client IP
iVISTA 4.1	None	80/server IP
Microsoft Xbox Live[7]	None	N/A

[1] Since SUA enables your LAN to appear as a single computer to the Internet, it is not possible to configure similar servers on the same LAN behind SUA. For example, you can have two WEB servers using TCP:80 in the same LAN. They must have different port numbers.

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

[3] In SUA mode, the remote NetMeeting user is allowed to connect only one local user, it is because the outsiders can not distinguish

between local users using the same internet IP. However, the local user can connect to multiple remote users.

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

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

[6] Prestige series support MSN Messenger 4.6/ 4.7/ 5.0 video/ voice pass-through NAT. In addition, for the Windows OS supported UPnP (Universal Plug and Play), such as Windows XP and Windows ME, UPnP supported in Prestige is an alternative solution to pass through MSN Messenger video/ voice traffic. The following model and firmware support UPnP function. For mote detail, please refer to UPnP application note.

[7] Prestige series support Microsoft Xbox Live since V3.52 firmware version. If your firmware is too old to support such function, you may have a work-around solution, please refer to ZyXEL website -> Support -> Xbox Live service http://www.zyxel.com/support/xbox.htm

- Notes

1. In 1.5x and 2.2x versions, if a SMTP (port 25) server is configured in menu 15 the POP3 (port 110) packets will also be forwarded to the same SMTP server by the Prestige automatically. There is no need to configure additional POP3 server in menu 15, unlike 2.2x and 1.5x versions, SMTP & POP3 servers are handled by the Prestige separately in V2.3 and above versions. So, two ports (25 & 110) must be configured in menu 15 to support both SMTP and POP3 services.
2. NetMeeting, RealPlayer, IP/TV and Quick Time are supported in V2.3 and above versions.

- Configurations

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

```
                Menu 15 - SUA Server Setup


          Port #         IP  Address
          ------       ---------------
        1.Default      192.168.1.34
        2. 0           0.0.0.0
        3. 0           0.0.0.0
        4. 0           0.0.0.0
        5. 0           0.0.0.0
        6. 0           0.0.0.0
        7. 0           0.0.0.0
        8. 0           0.0.0.0
```

Using UPnP

---

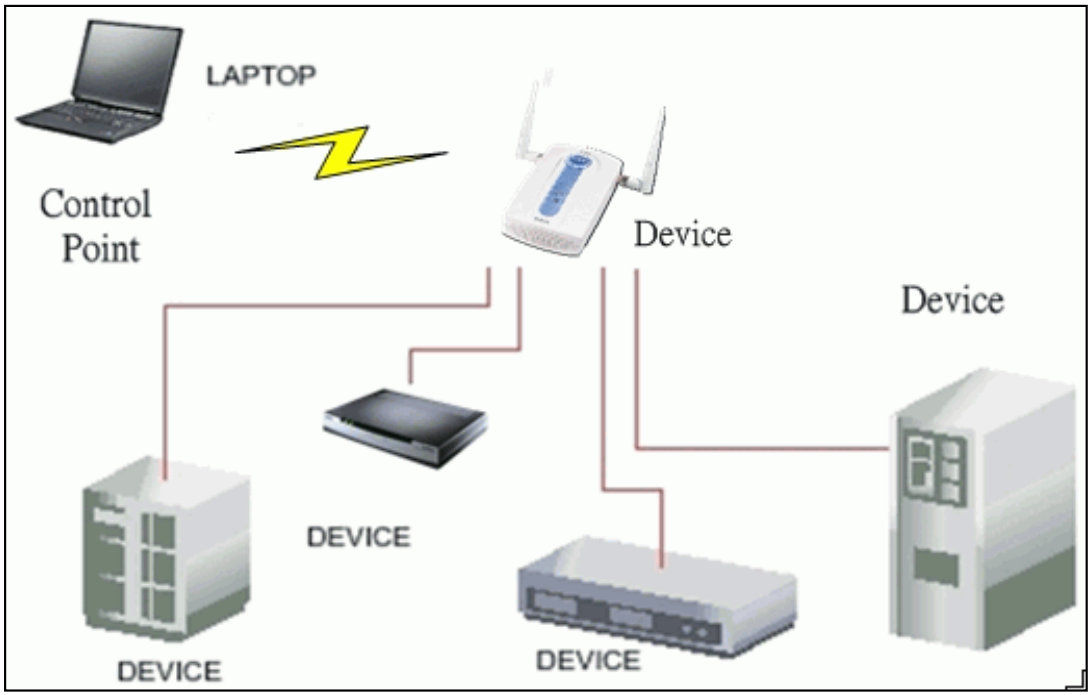
1. What is UPnP

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 ¡V 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 devices 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 it's 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.

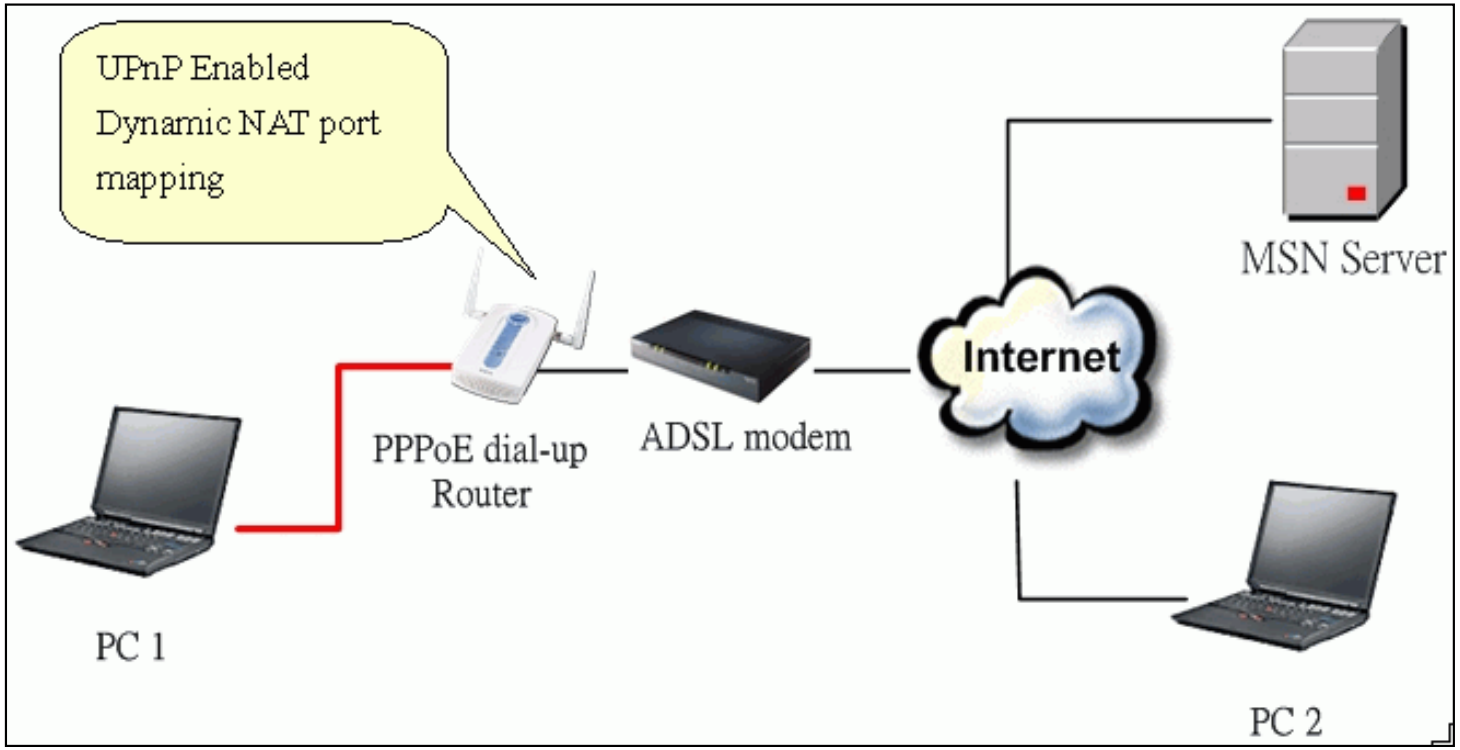
---

2. Use 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.



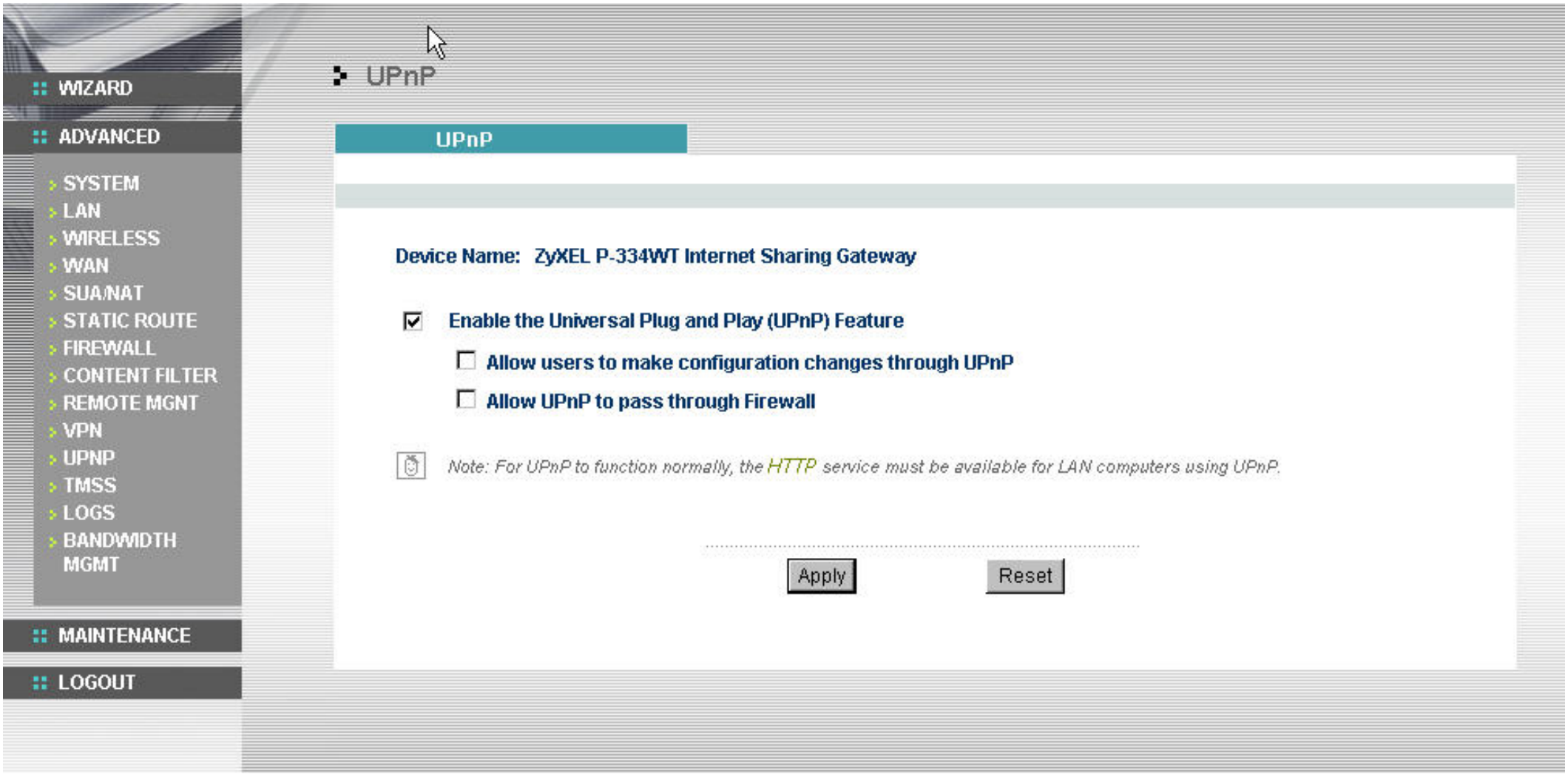
Device: PPPoE Dial-up Router
Service: NAT function provided by PPPoE Dial-up Router
Control Point: PC1

1. Enable UPnP function in ZyXEL device

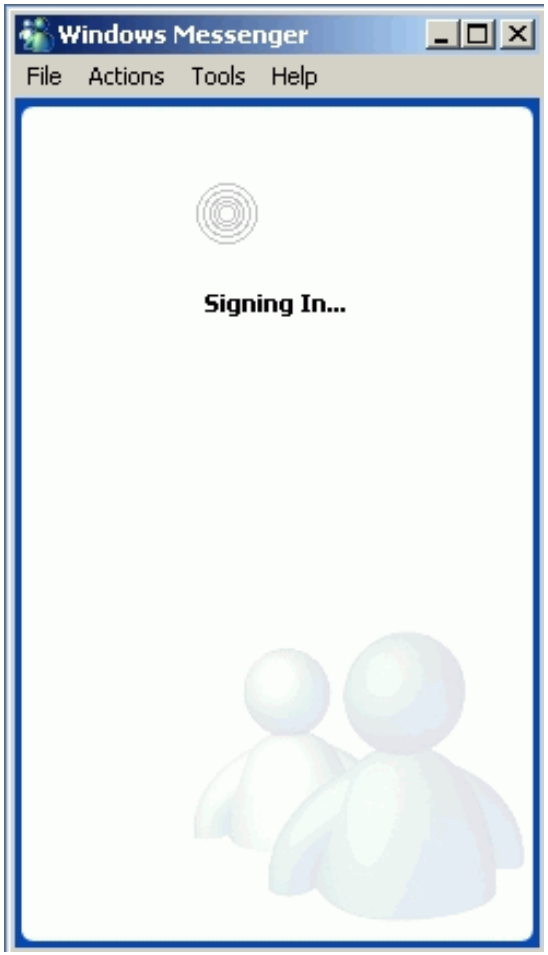
Go to **Advanced->UPnP**, check two boxes, **Enable PnP feature** and **Allow users to make...**

The first check box enables UPnP function in this device.

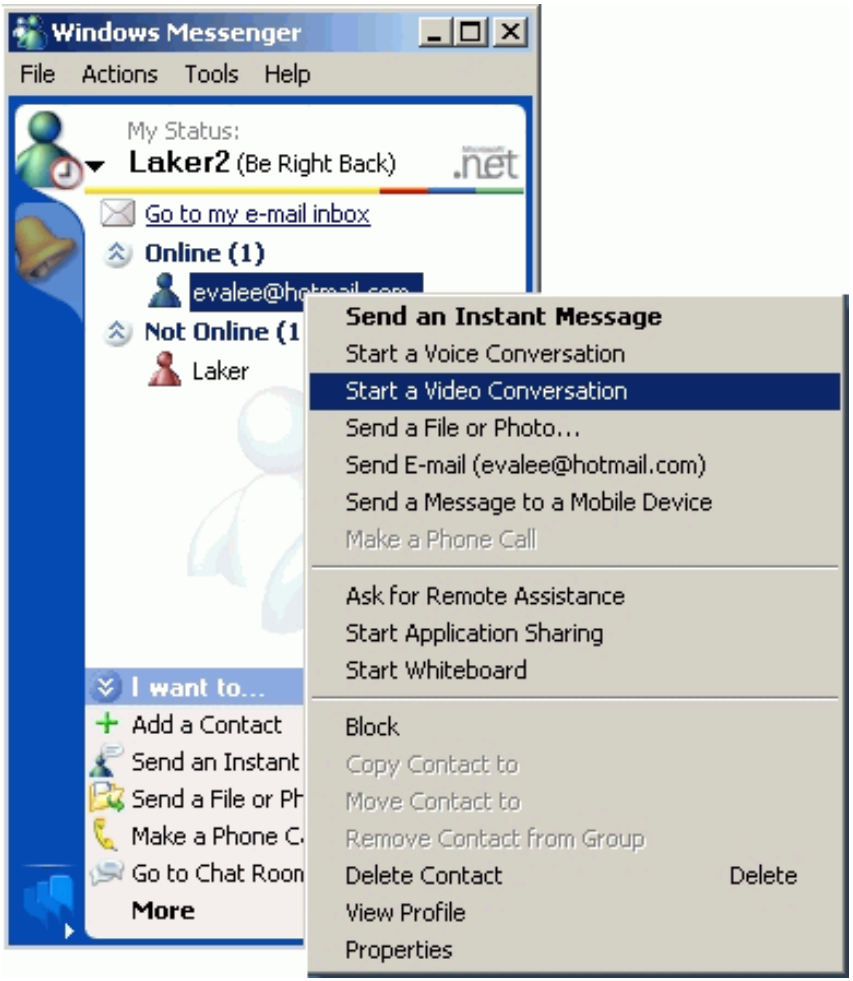
The second check box allow users' application to change configuration in this device. For instance, if you enable this item, then user's MSN application can assign dynamic port mapping to the router. So that network administrator don't need to setup SUA port mapping in the router.



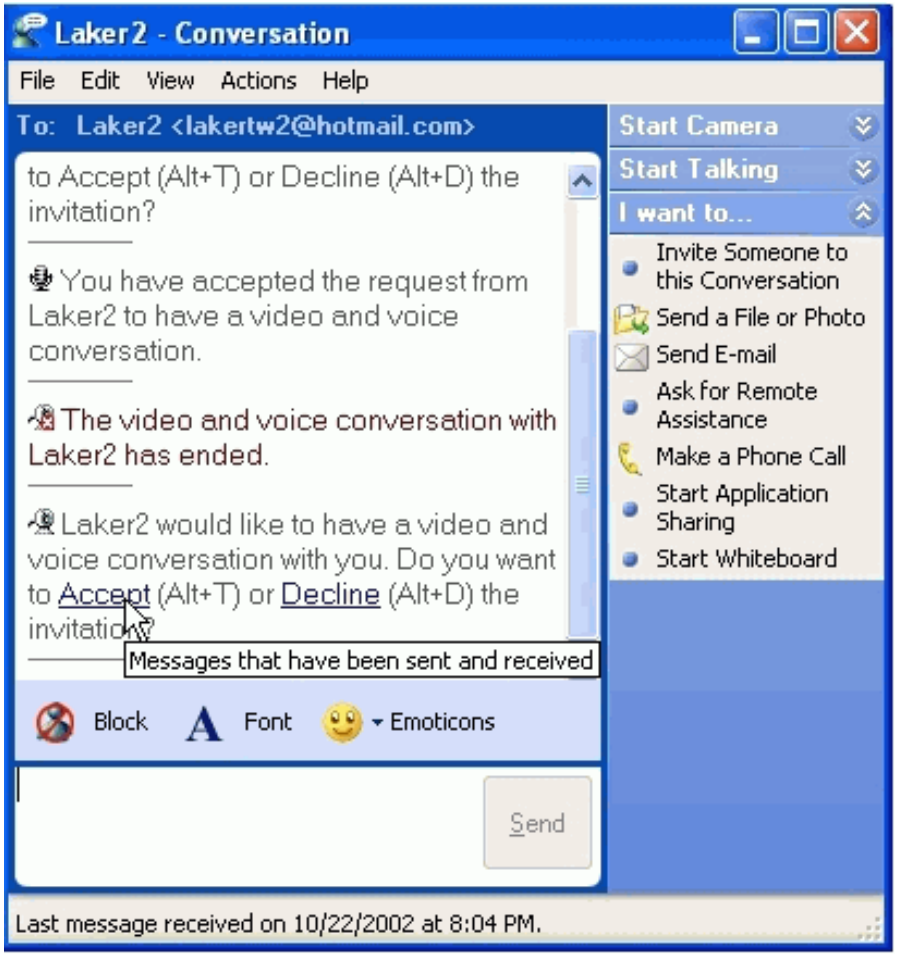
2. After getting IP address, you can go to open MSN application on PC and sign in MSN server.



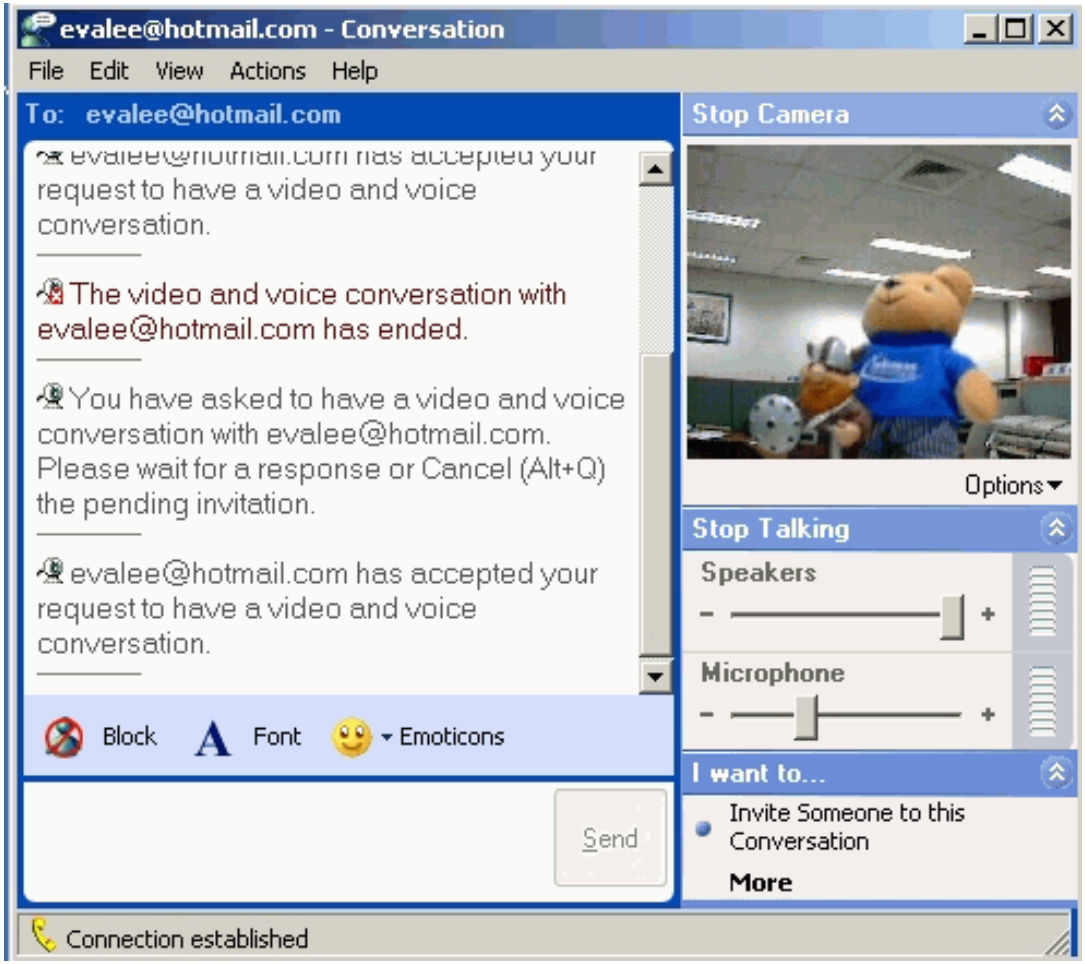
3. Start a Video conversation with one online user.



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



5. Finally, your video conversation is achieved.



---

3. View dynamic ports opened by UPnP

When using UPnP, if the ZyXEL device is configured as "**Allow users to make configuration changes through UPnP**", the device will accept any port opening request sent by UPnP protocol. And actually, such behaviour also add some risks to your internal LAN. For security sake, we provide a CI command for users to view currently opened ports.

Please go to SMT menu, and type this command, "**ip nat server disp**" to display the dynamic port mappings. Please note that, the UPnP dynamic port mappings start from item 13 to 35.

```
ras> ip nat server disp
Server Set: 1
Rule         name              Svr P Range    Server IP       LeasedTime
     Active  protocol    Int Svr P Range    Remote Host IP Range
-------------------------------------------------
   1 DMZ                       default             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   2                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   3                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   4                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   5                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   6                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   7                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   8                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   7                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   8                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
   9                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
  10                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
  11                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
  12                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
  13 msnmsgr (192.168.1.33:12288) 35   35313 - 35313     192.168.1.33   0
     YES      UDP           12288 - 12288          0.0.0.0 - 0.0.0.0
  14 msnmsgr (192.168.1.33:7173) 360   36061 - 36061     192.168.1.33   0
     YES      TCP            7173 - 7173           0.0.0.0 - 0.0.0.0
  15                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
  16                             0 - 0             0.0.0.0   0
      No      ALL                0 - 0             0.0.0.0 - 0.0.0.0
  17                             0 - 0             0.0.0.0   0
```

```
      No      ALL                0 - 0              0.0.0.0 - 0.0.0.0
  18                             0 - 0              0.0.0.0   0
<deleted...>
```

Filter

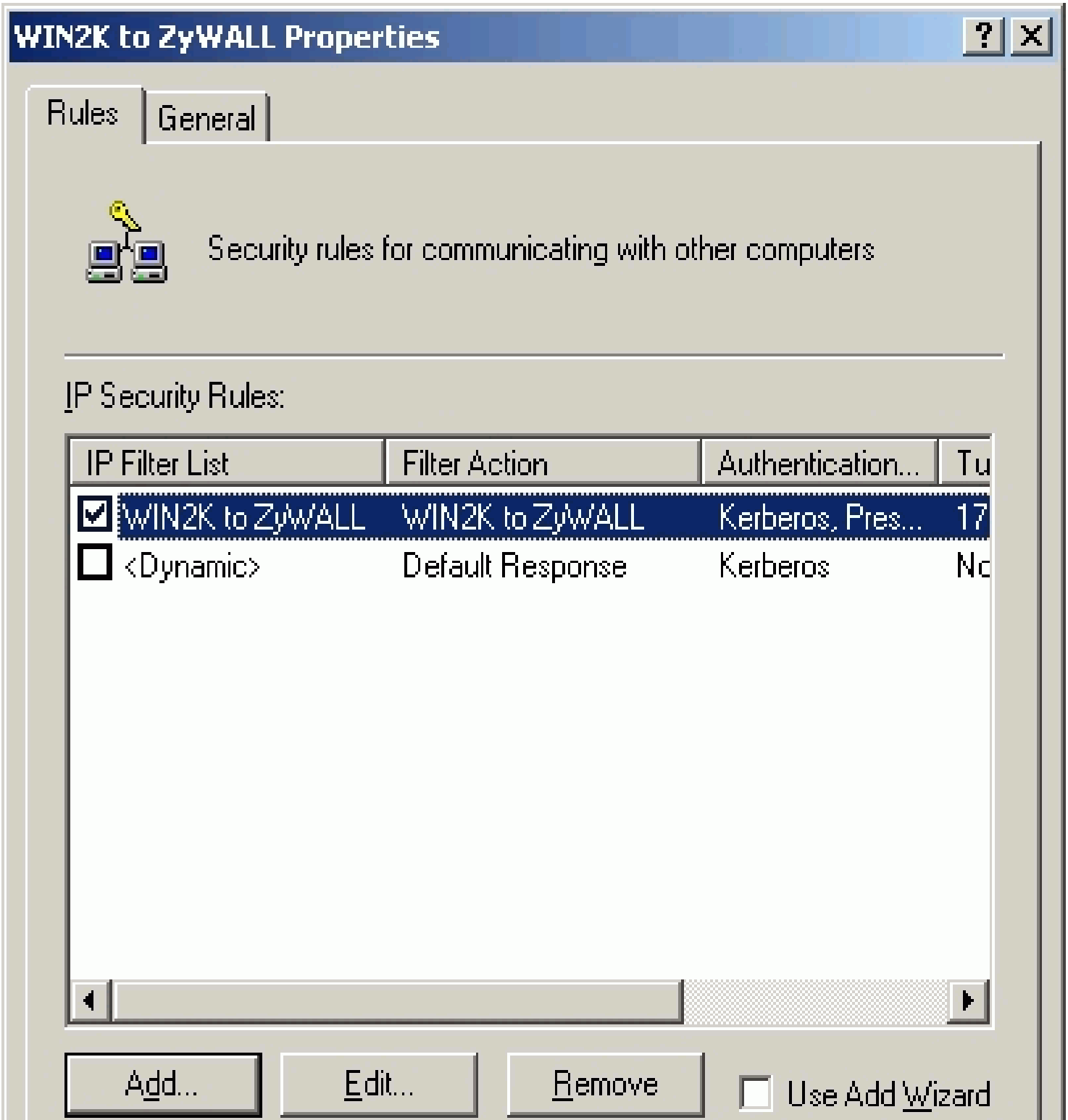
- How does ZyXEL filter work?
- Filter Examples
  - A filter for blocking the web service
  - A Filter for blocking the FTP connection from WAN
  - A filter for blocking a specific client
  - A filter for blocking a specific MAC address
  - A filter for blocking the NetBIOS packets

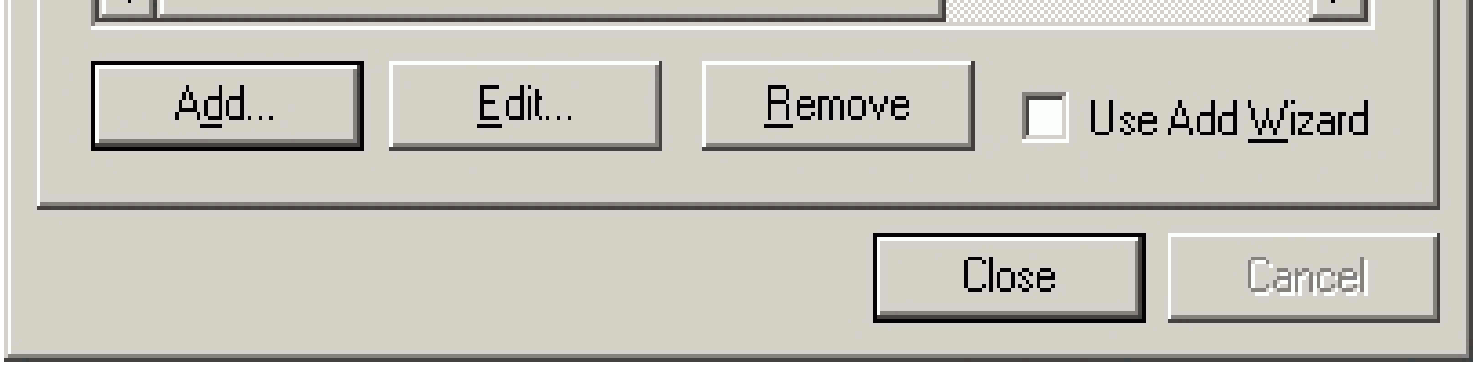
Filter

How does ZyXEL filter work?

- **Filter Structure**

The P334WT 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 P334WT is receiving and sending the packets; i.e. the ISDN interface. So, the execution sequence has to be changed. The logic flow of the filter is shown in Figure 1 and the sequence of the logic flow for the packet from LAN to WAN is:

1. LAN device and protocol input filter sets.
2. WAN protocol call and output filter sets.
3. 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.
4. WAN device output and call filter sets.

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

5. WAN device input filter sets.
6. 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.
7. WAN protocol input filter sets.
8. LAN device and protocol output filter sets.

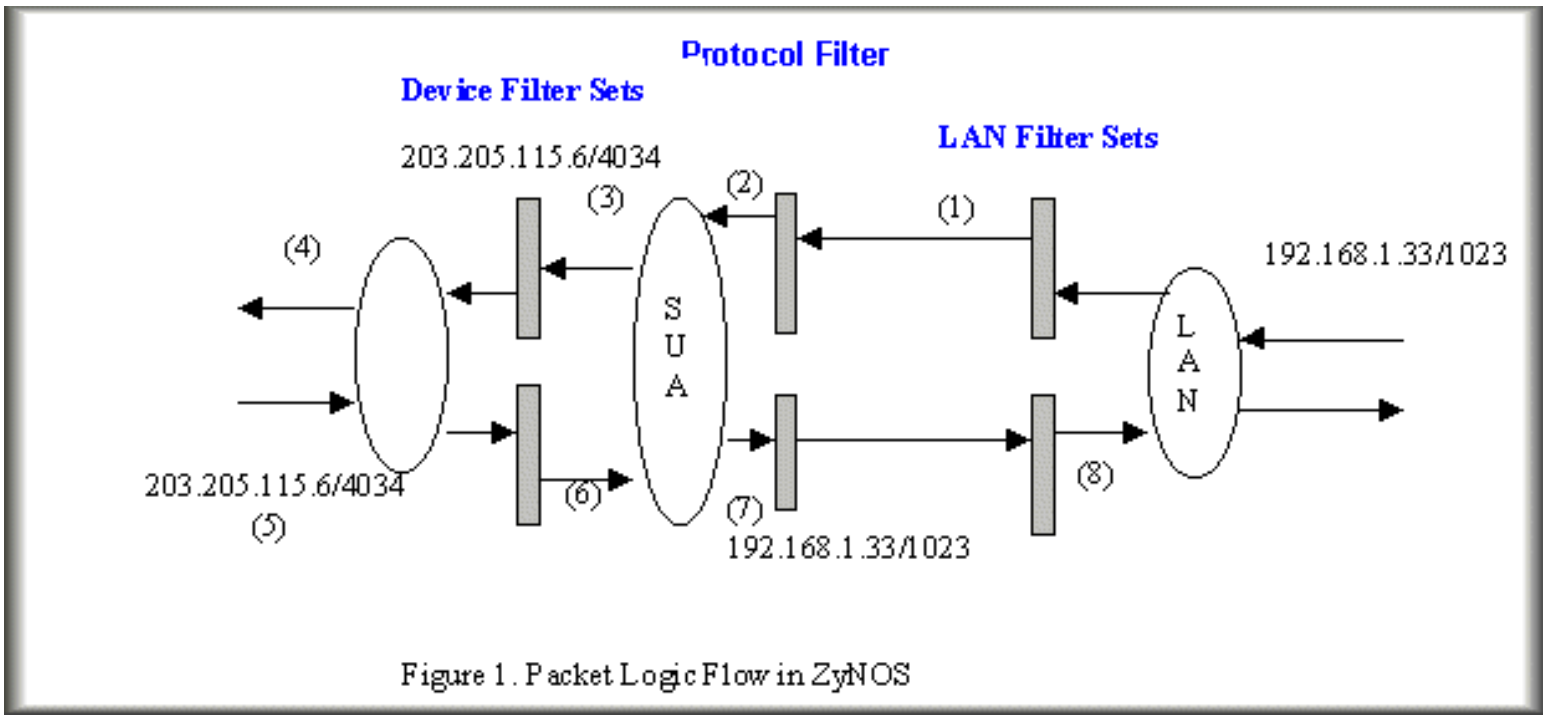


Figure 1. Packet Logic Flow in ZyNOS

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

Menu 21.1.1:

```
                Menu 21.1.1 - Generic Filter Rule

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

Menu 21.1.2:

```
                    Menu 21.1.2 - TCP/IP Filter Rule

                  Filter #: 1,2
                  Filter Type= TCP/IP Filter Rule
                  Active= Yes
                  IP Protocol= 0   IP Source Route= No
                  Destination: IP Addr= 0.0.0.0
                               IP Mask= 0.0.0.0
                               Port #= 0
                               Port # Comp= None
                       Source: IP Addr= 0.0.0.0
                               IP Mask= 0.0.0.0
                               Port #= 0
                               Port # Comp= None
                  TCP Estab= N/A
                  More= No          Log= None
                  Action Matched= Check Next Rule
                  Action Not Matched= Check Next Rule

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

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

Menu 3.1:

```
                  Menu 3.1 - General Ethernet Setup

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

Menu 11.1:

```
                Menu 11.1 - Remote Node Profile

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

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


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

Menu 11.5:

```
                    Menu 11.5 - Remote Node Filter

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

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

In order to avoid operational problems later, the P334WT will disable its routing/bridging functions if there is an inconsistency among its filter rules.

Filter Example

A filter for blocking the web service

- Configuration

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

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

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

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

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

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

1. Create a filter set in Menu 21

```
                    Menu 21 - Filter Set Configuration

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


                  Enter Filter Set Number to Configure= 1

                  Edit Comments=

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

2. Rule 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 in the 'Output Protocol Filter Set' of menu 11.5 for activating it.

```
                    Menu 11.5 - Remote Node Filter

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



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

Filter Example

A filter for blocking the FTP connections from WAN

- Introduction

The P334WT supports the firmware and configuration files upload using FTP connections via LAN and WAN. So, it is possible that anyone can make a FTP connection over the Internet to your P334WT. To prevent outside users from connecting to your P334WT via FTP, you can configure a filter to block FTP connections from WAN.

- Before you begin

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

1. **The inbound packet type (protocol & port number):** In this case, it is **TCP(06)** protocol with port **20 or 21**.
2. **The source IP address:** In this case, we block all connections from outside so the source IP is **0.0.0.0**.
3. **The destination IP address:** It is the P334WT's IP address, but it is not available in SUA case since most WAN IP address is dynamically assigned by the ISP. So, we can only enter **0.0.0.0** as the destination IP in the filter rule. Once 0.0.0.0 is set as the destination IP, no FTP connections are allowed to reach the P334WT nor the FTP server on the LAN. For the LAN-to-LAN connection, you enter the P334WT's LAN IP as the destination IP in the filter rule. After the FTP filter is applied to the remote node, it only blocks the FTP connection to the P334WT but still permits the FTP connection to the local FTP server.

- Configuration
    - Create a filter set in Menu 21, e.g., set 4
    - Create two filter rules in Menu 21.4.1 and Menu 21.4.2
        - Rule 1- block the inbound FTP packet, TCP (06) protocol with port number 20
        - Rule 2- block the inbound FTP packet, TCP (06) protocol with port number 21
    - Apply the filter set in remote node, Menu 11

- Create a filter set in Menu 21

```
                    Menu 21 - Filter Set Configuration

     Filter                                  Filter
     Set #        Comments                   Set #
Comments
     ------  -----------------               ------
-----------------
       1      NetBIOS_WAN                      7
_______________
       2      NetBIOS_LAN                      8
_______________
       3      Telnet_WAN                       9
_______________
       4      FTP_WAN                          10
_______________
       5      _______________                  11
_______________
       6      _______________                  12
_______________



                  Enter Filter Set Number to Configure= 4

                  Edit Comments= FTP_WAN

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

- Rule 1- block the inbound FTP packet, TCP (06) protocol with port number 20

```
                      Menu 21.4.1 - TCP/IP Filter Rule

                  Filter #: 4,1
                  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 #= 20
                               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:
```

- Rule 2- block the inbound FTP packet, TCP (06) protocol with port number 21

```
                Menu 21.4.2 - TCP/IP Filter Rule

Filter #: 4,2
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 #= 21
             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:
```

- When two rules are completed, you can see the rule summary in Menu 21.1

```
                    Menu 21.4 - 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=20            N D N
2 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21            N D F
3 N
4 N
5 N
6 N
```

- Choose the remote node number where you want to block the inbound FTP connections and apply the filter set in menu 11.5 by selecting the '**Edit Filter Sets**' to '**Yes**'.

- Put the filter set number **'4'** to the **'Input Protocol Filter Set'** in menu 11.5 for activating the FTP_WAN filter.

```
                      Menu 11.5 - Remote Node Filter

                  Input Filter Sets:
                    protocol filters= 4
                      device filters=
                  Output Filter Sets:
                    protocol filters=
                      device filters=
```

Filter Example

A filter for blocking a specific client

Configuration

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

```
                    Menu 21 - Filter Set Configuration

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



                 Enter Filter Set Number to Configure= 0

                 Edit Comments=

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

2. One rule for blocking all packets from this client

```
                    Menu 21.1.1 - TCP/IP Filter Rule

               Filter #: 1,1
               Filter Type= TCP/IP Filter Rule
               Active= Yes
               IP Protocol= 0     IP Source Route= No
               Destination: IP Addr= 0.0.0.0
                            IP Mask= 0.0.0.0
                            Port #=
                            Port # Comp= None
                    Source: IP Addr= 192.168.1.5
                            IP Mask= 255.255.255.255
                            Port #=
                            Port # Comp= None
               TCP Estab= N/A
               More= No            Log= None
               Action Matched= Drop
               Action Not Matched= Forward

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

Key Settings:

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

3. Apply the filter set number '1' in the **'Output Protocol Filter Set'** field of SMT menu 11.5 for activating it.

```
                Menu 11.5 - Remote Node Filter

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



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

After this filter set is applied to this field, the client (192.168.1.5) will not be allowed to access the Internet.

Filter Example

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 324 you can identify the uninteresting MAC address from the Prestige 324'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 324……

ras> sys trcp sw off
ras> sys trcp disp

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

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

The detailed format of the Ethernet Version II:

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

Configurations

From the above first trace, we know a client is trying to ping request the Prestige 324 router. And from the second trace, we know the Prestige 324 router will send a reply to the client accordingly. The following sample filter will utilize the 'Generic Filter Rule' to block the MAC address **[00 80 c8 4c ea 63]**.

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

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

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

```
                Menu 21.1.1 - Generic Filter Rule

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

Key Settings:

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

- Active
  Turn 'Active' to 'Yes'

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

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

- Mask (in hexadecimal)
  Specify the value that the Prestige 324 will logically qualify (logical AND) the data in the packet.
  Since the Length is set to 6 octets the Mask for it should be 12 hexadecimal numbers. In this case, we intent to set to 'ffffffffffff' to mask the incoming source MAC address, [00 80 c8 4c ea 63].

- Value (in hexadecimal)
  Specify the MAC address **[00 80 c8 4c ea 63]** that the Prestige 324 should use to compare with the masked packet. If the result from the masked packet matches the 'Value', then the packet is considered matched.

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

it.

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

```
                Menu 21.1.2 - Generic Filter Rule

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

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

```
              Menu 3.1 - General Ethernet Setup

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

Filter Example

A filter for blocking the NetBIOS packets

- Introduction

The NETBIOS protocol is used to share a Microsoft comupter of a workgroup. For the security concern, the NetBIOS connection to a outside host is blocked by Prestige 324 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 menu 11.5 for activating it.

```
                  Menu 11.5 - Remote Node Filter

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



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

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:
```

- 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
```

- 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=
```

Setting Up the Syslog

The Prestige is able to send four types of system log to a Syslog deamon such as Unix Syslogd.

- **Prestige Setup**

```
Menu 24.3.2 - System Maintenance - Syslog Logging

                Syslog:
                Active= Yes
                Syslog Server IP Address= 192.168.1.34
                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.

- **UNIX Setup**

1. Make sure that your syslogd is started 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.

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 SNMPv2. 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:

1. Reads

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

2. Writes

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

3. 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.

4. Traps

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

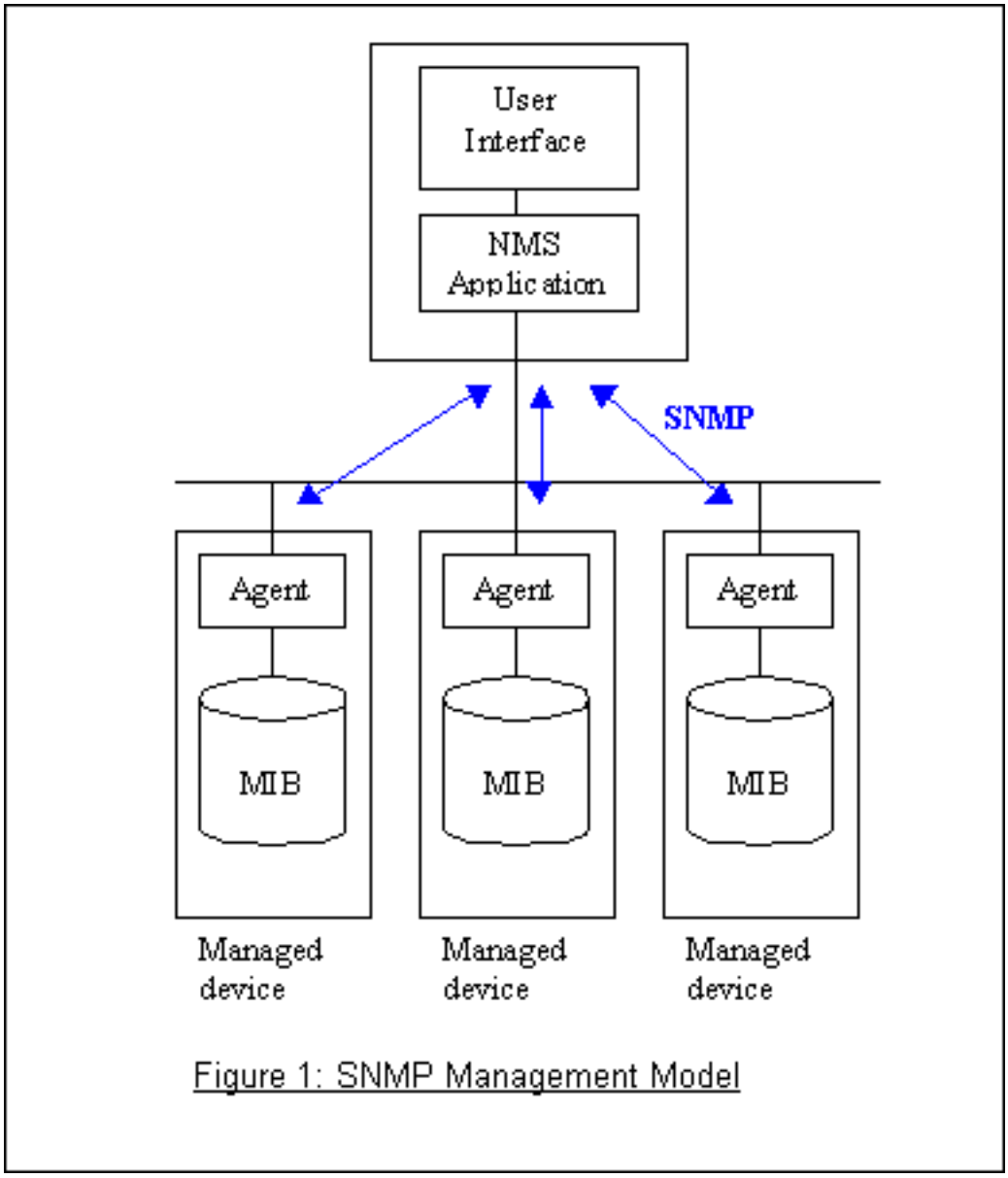


Figure 1: SNMP Management Model

---

2. 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. Further, users can also add ZyXEL's private MIB in the NMS to monitor and control additional system variables. The ZyXEL's private MIB tree is shown in figure 3. For SNMPv2 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

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

1. coldStart (defined in RFC-1215) :

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

2. warmStart (defined in RFC-1215) :

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

3. 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.

4. 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.

5. authenticationFailure (defined in RFC-1215) :

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

6. whyReboot (defined in ZYXEL-MIB) :

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

   (i) For intentional reboot :

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

   (ii) For fatal error :

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

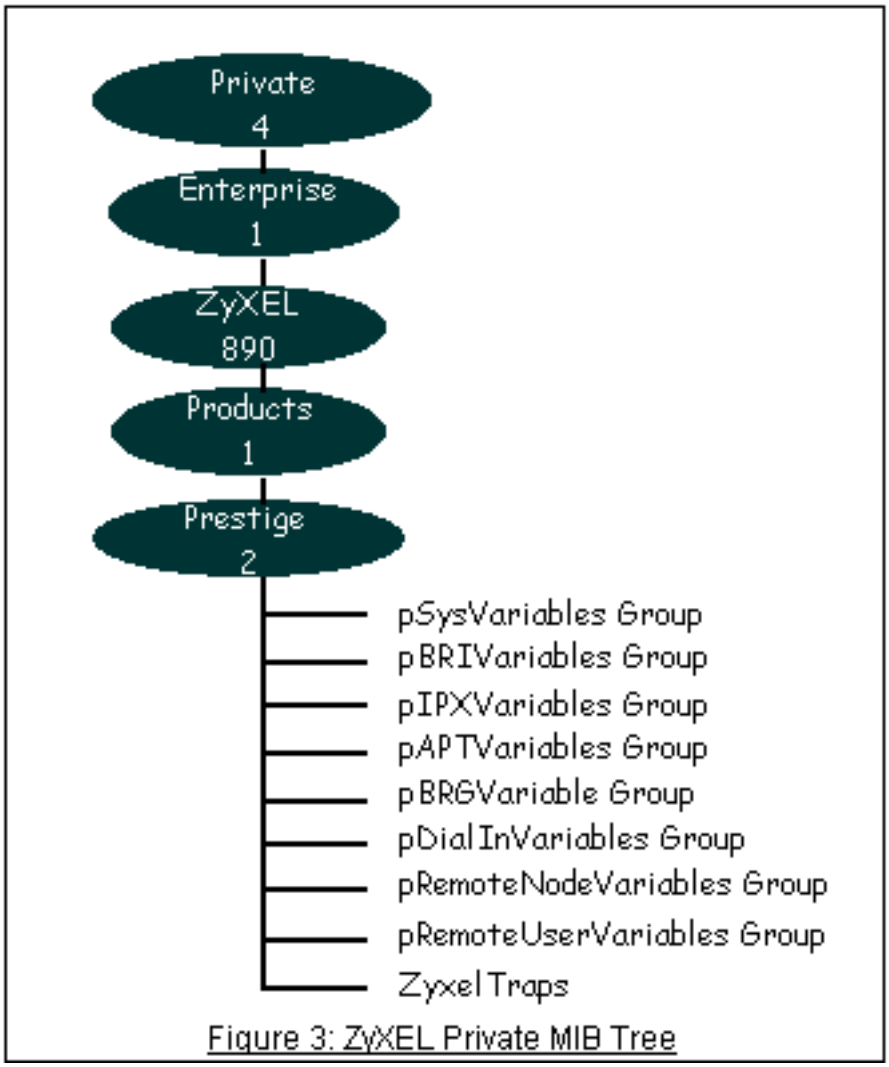
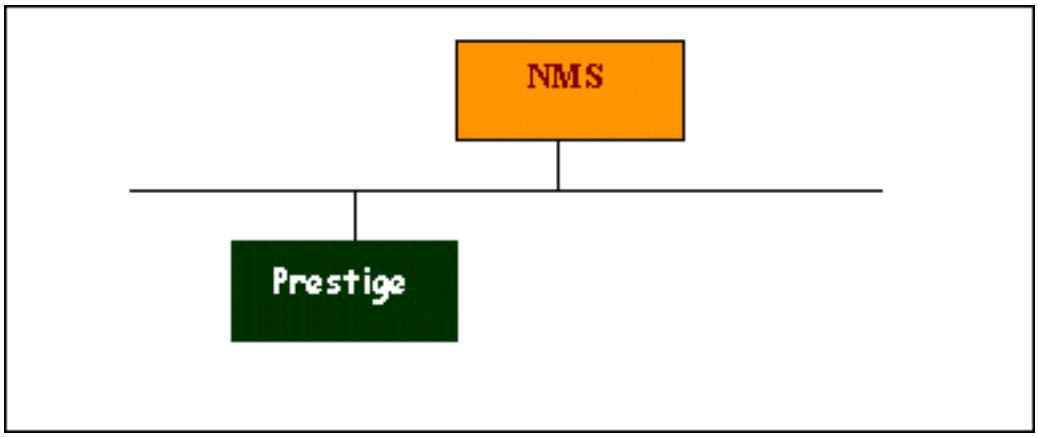


Figure 3: ZyXEL Private MIB Tree

---

3. 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
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
Trusted Host	Enter the IP address of the NMS. The Prestige will only respond to SNMP messages coming from this IP address. **If 0.0.0.0 is entered, the Prestige will respond to all NMS managers.**
Trap Community	Enter the community name in each sent trap to the NMS. This Trap Community must match what the NMS is expecting. The default is 'public'.
Trap Destination	Enter the IP address of the NMS that you wish to send the traps to. **If 0.0.0.0 is entered, the Prestige will not send trap any NMS manager.**

Using the Dynamic DNS (DDNS)

- What is DDNS?

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

Without DDNS, we always tell the users to use the WAN IP of the 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) 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 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) 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 where you apply the DNS from and update the WAN IP to.

- Setup the DDNS

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

```
                Menu 1 - General Setup

          System Name= P334WT
          Domain Name=



          First System DNS Server= From ISP
          IP Address= N/A
          Second System DNS Server= From ISP
          IP Address= N/A
          Third System DNS Server= From ISP
          IP Address= N/A
          Edit Dynamic DNS= Yes
```

```
                Menu 1.1 - Configure Dynamic
          DNS

               Service Provider= WWW.DynDNS.ORG
               Active= Yes
               Host Name 1=
               Host Name 2=
               Host Name 3=
               Username=
               Password= ********
               Enable Wildcard Option= No
               Enable Off Line Option= N/A
               IP Address Update Policy:
               DDNS Server Auto Detect IP
          Address= No
               Use Specified IP Address= No
               Use IP Address= N/A
```

Key Settings for using DDNS function:

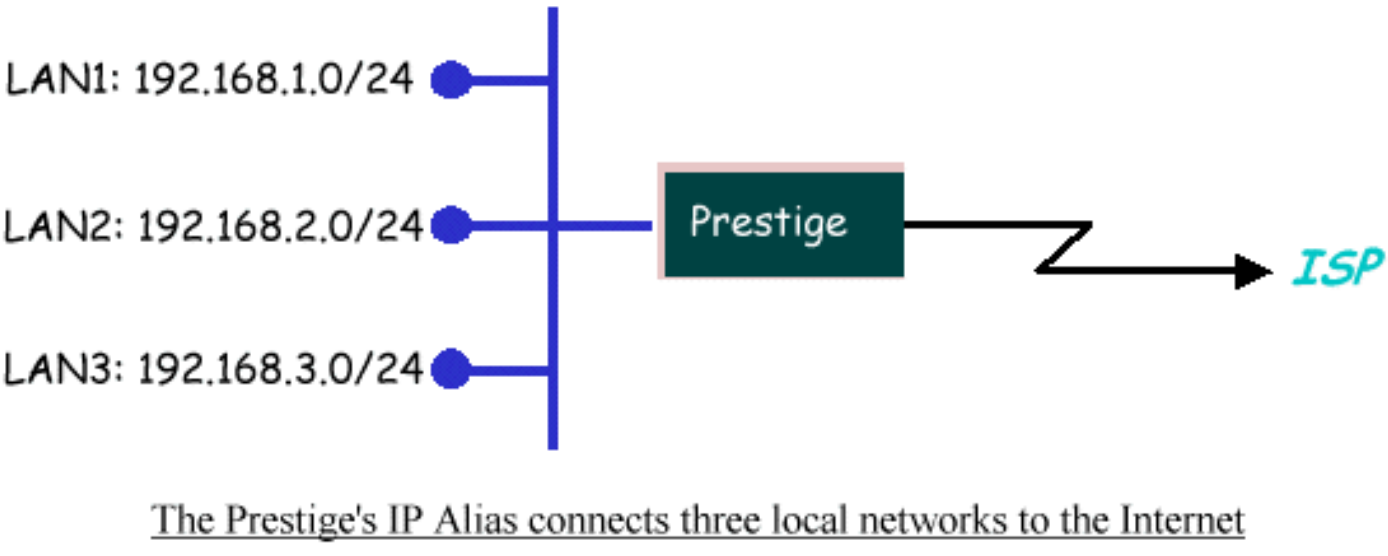
Option	Description
Service Provider	Enter the DDNS server in this field. Currently, we support WWW.DYNDNS.ORG.

Active	Toggle to '**Yes**'.
Host	Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw.
User	Enter the user name that
Password	Enter the password that the DDNS server gives to you.
Enable Wildcard	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is WWW.DYNDNS.ORG.

Using IP Alias

- What is IP Alias ?

In a typical environment, a LAN router is required to connect two local networks. The Prestige supports to 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's IP Alias connects three local networks to the Internet

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 Prestigeto 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 - 1999 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 Ethernet Setup


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

Key Settings:

DHCP Setup	If the Prestige's DHCP server is enabled, the IP pool for the clients can be any of the three networks.
TCP/IP Setup	Enter the first LAN IP address for the Prestige. This will create the first route in the enif0 interface.
Edit IP Alias	Toggle to **'Yes'** to enter menu 3.2.1 for setting up the second and third networks.

2. Edit the second and third networks in menu 3.2.1 by configuring the 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:

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

Using FTP to Upload the Firmware and Configuration Files

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

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

1. **Using FTP command in terminal**
2. **Using FTP client software**

---

1. **Using FTP command in terminal**

Step 1	Use FTP client from your workstation to connect to the Prestige by entering the IP address of the Prestige.
Step 2	Press '**Enter**' key to ignore the username, because the Prestige does not check the username.
Step 3	Enter the SMT password as the FTP login password, the default is '**1234**'.
Step 4	Enter command '**bin**' to set the transfer type to binary.
Step 5	Use '**put**' command to transfer the file to the Prestige.

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

Example:

```
C:\temp>ftp 202.132.155.97
Connected to 202.132.155.97.
220 FTP version 1.0 ready at Thu Jan 1 00:02:09 1970
User (202.132.155.97:(none)):  <Enter>
331 Enter PASS command
Password:****
230 Logged in
ftp> bin
200 Type I OK
ftp> put p312.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 924512 bytes sent in 4.83Seconds 191.41Kbytes/sec.
ftp>
```

Here, the '**p312.bin**' is the local file and '**ras**' is the remote file that will be saved in the Prestige.

The Prestige reboots automatically after the uploading is finished.

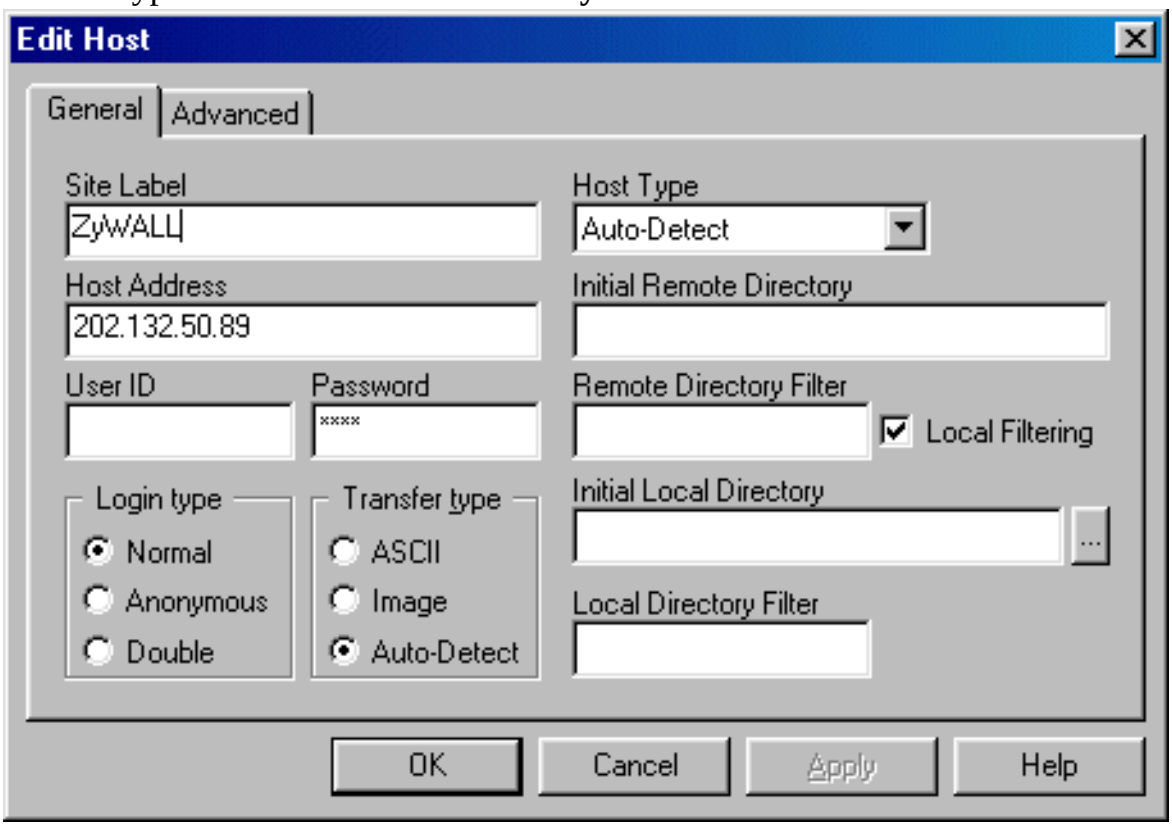
---

2. **Using FTP client software**

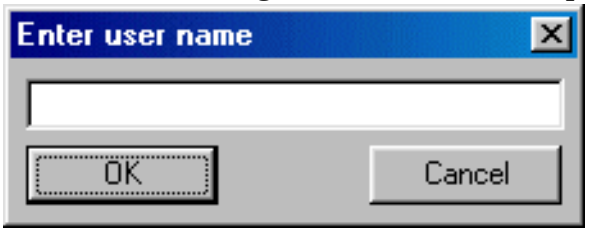
Step 1	Rename the local firmware and configuration files to **'ras'** and **'rom-0'**, because we can not specify the remote file name in the FTP client software.
Step 2	Use FTP client from your workstation to connect to the Prestige by entering the IP address of the Prestige.
Step 3	Enter the SMT password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

Example:

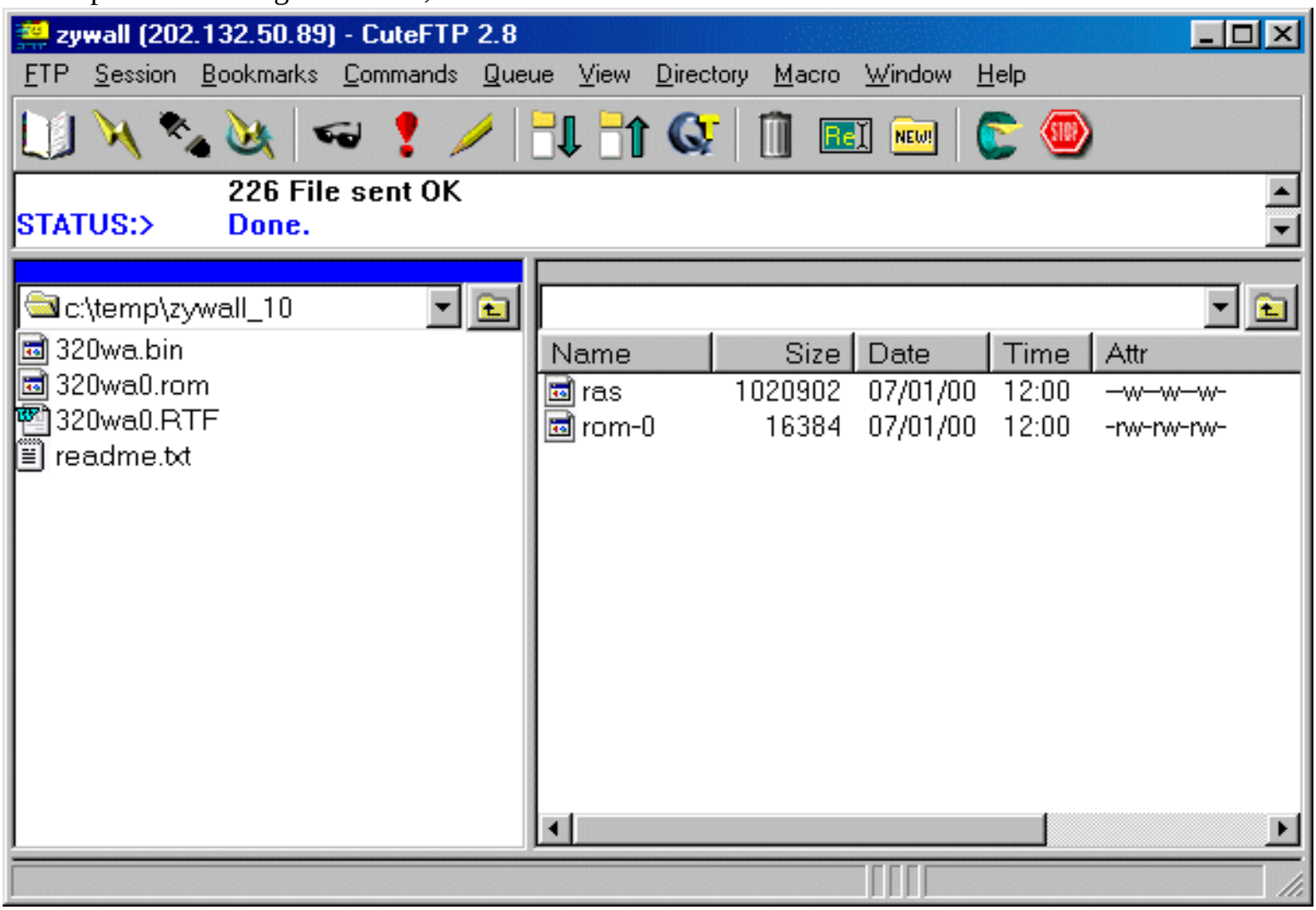
1. Connect to the Prestige by entering the Prestige's IP and SMT password in the FTP software. Set the transfer type to **'Auto-Detect'** or **'Binary'**.



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



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



4.The Prestige reboots automatically after the uploading is finished.

Firmware/Configurations Uploading and Downloading using TFTP

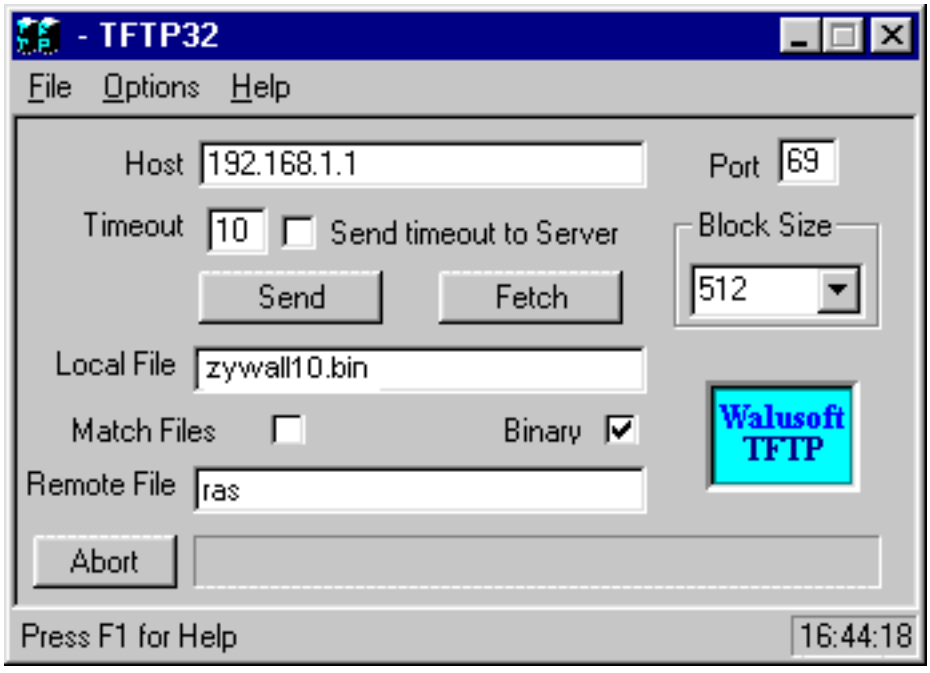
- Using TFTP client software
- Using TFTP command on Windows NT
- Using TFTP command on UNIX
- Downloading Walusoft TFTP from http://www.walusoft.co.uk

- **Using TFTP client software**
  - **Upload/download ZyNOS via LAN**
  - **Upload/download SMT configurations via LAN**

Using TFTP to upload/download ZyNOS via LAN

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

An example:



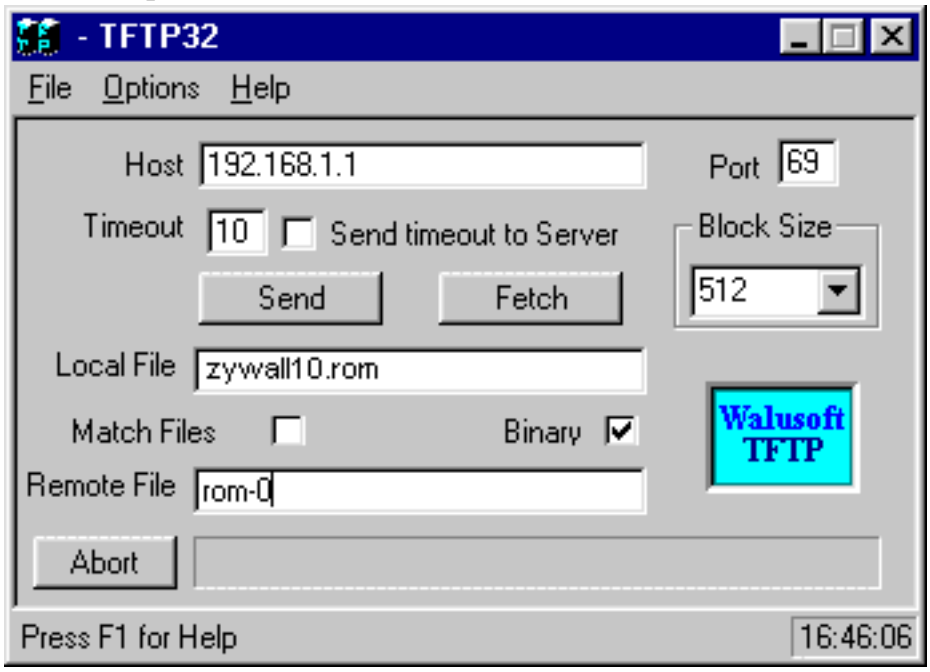
The 192.168.1.1 is the IP address of the Prestige. The local file is the source file of the ZyNOS

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

Using TFTP to upload/download SMT configurations via LAN

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

An Example:



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

- **Using TFTP command on Windows NT**

Before you begin:

1. TELNET to your Prestige first before using TFTP command

2. Type the CI command '**sys stdio 0**' to disable console idle timeout in Menu 24.8 and stay in Menu 24.8

    - **Upload ZyNOS via LAN**

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

    - **Download ZyNOS via LAN**

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

    - **Upload SMT configurations via LAN**

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

    - **Download SMT configurations via LAN**

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

- **Using TFTP command on UNIX**

Before you begin:

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

Example:

```
[cppwu@faelinux cppwu]$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

Password: ****

                Copyright (c) 1994 - 2004 ZyXEL Communications
Corp.

                          Prestige 334WT Main Menu

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

                                         99. Exit


                       Enter Menu Selection Number: 24


                     Menu 24 - System
                     Maintenance

                     1. System Status
                     2. System
                     Information and
                     Console Port Speed
                     3. Log and Trace
                     4. Diagnostic
                     5. Backup
                     Configuration
```

```
                        6. Restore
                        Configuration
                        7. Firmware Upload
                        8. Command
                        Interpreter Mode
                        9. Call Control
                        10. Time and Date
                        Setting
                        11. Remote
                        Management Setup


                         Enter Menu Selection Number: 8

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> sys stdio 0
ras> (press Ctrl+] to escape to Telnet prompt)
telnet> z
[1]+  Stopped                 telnet 192.168.1.1
[cppwu@faelinux cppwu]$ tftp
tftp> connect 192.168.1.1
tftp> binary                      <- change to binary mode
tftp> get rom-0 [local-rom]       <- download configurations
tftp> get ras [local-firmware]    <- download firmware
tftp> put [local-rom] rom-0       <- upload configurations
tftp> put [local-firmware] ras    <- upload firmware
```

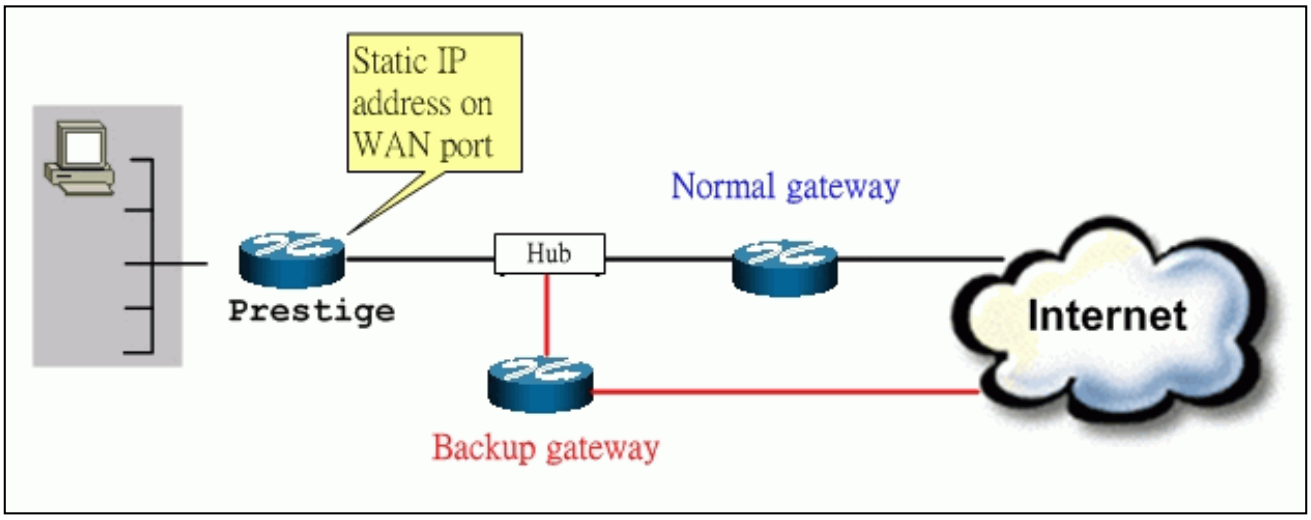
Using Traffic Redirect

- What is Traffic Redirect ?

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

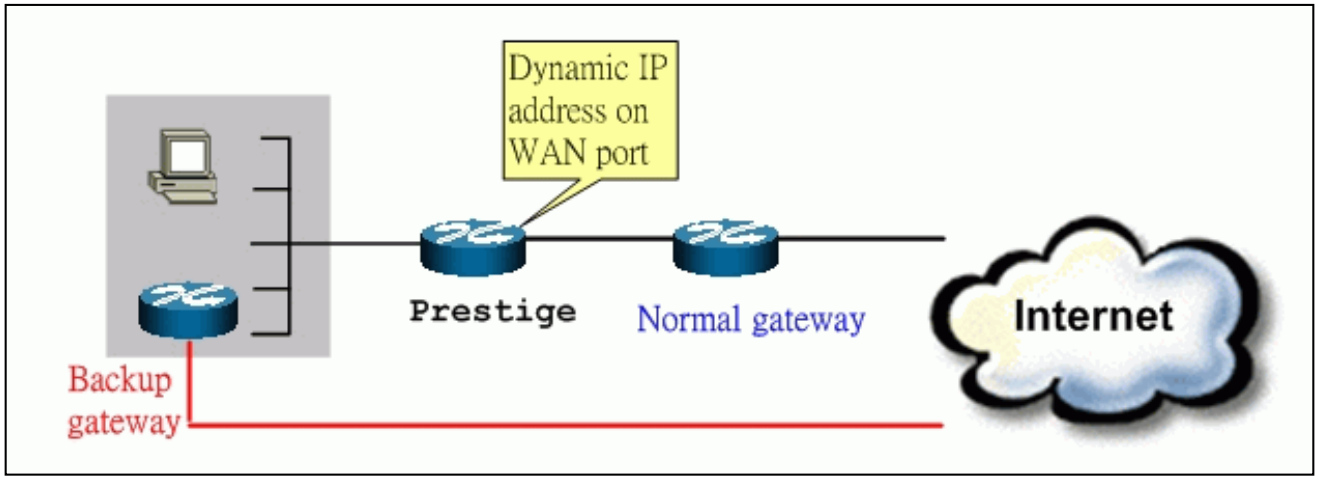
- How to deploy backup gateway?

You can deploy the backup gateway on the WAN or LAN of Prestige. However, if you would like to deploy the backup gateway on the WAN of Prestige, please make sure that your Prestige has a static WAN IP address at first. Otherwise, we recommend you to deploy the backup gateway on the LAN of Prestige.



Traffic Redirect on WAN port

When Prestige has a dynamic IP address on it's WAN port, it may be easier to connect backup gateway to the 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 11.6-Traffic Redirect Setup.**

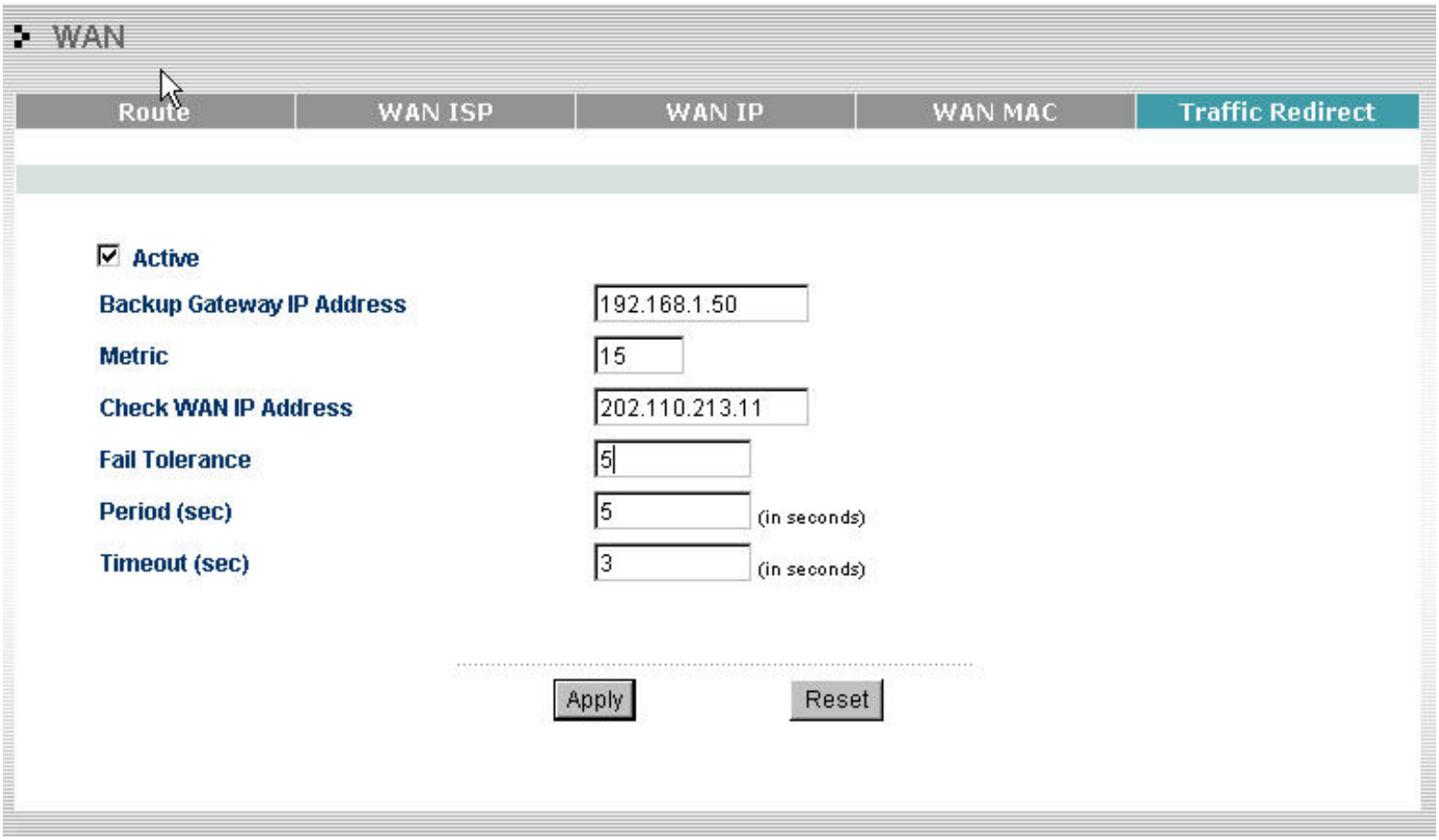
Menu 11.1 - Remote Node Profile

```
Menu 11.6 - Traffic Redirect Setup

Active= Yes
Configuration:
Backup Gateway IP Address= 192.168.1.50
Metric= 15
Check WAN IP Address= 202.132.154.1
Fail Tolerance= 5
Period(sec)= 30
Timeout(sec)= 2



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

Key Settings:

Active	Press [Space BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup.
Backup Gateway IP Address	The IP address of your backup gateway. Prestige automatically forwards outgoing traffic to this IP address if Prestige's Internet connection terminates.
Metric	Enter a number from 1 to 15 to give your traffic redirect route a priority number. The smaller the number, the higher priority the route has.
Check WAN IP Address	Configure a reliable server on Internet (for example, your ISP's DNS server address) for Prestige to check it's WAN connectivity periodically. If you leave this field as 0.0.0.0, Prestige will check it's default gateway IP address instead.
Fail Tolerance	Specify the number of times your Prestige may attempt and fail to connect to Internet before triggering traffic redirect connection.
Period	Specify the period that Prestige would check it's WAN connectivity.
Timeout	Specify the seconds that Prestige would wait for a response from the reliable server.

You can also configure traffic redirect via web configuration. The configuration page is in **ADVANCED/WAN/Traffic Redirect**.



- Are you using Prestige family?

In case your are using Presitge with firewall function turns on, it's strongly recommended that you deploy the backup gateway in IP alias segment. You can refer to here for how to use IP alias in Prestige, and firewall FAQ for the reason why we make such suggestion.

VPN Application Notes

- **Using P334WT IPSec VPN**
  - P334WT to ZyWALL Tunneling
  - Suecure Gateway with Dynamic WAN IP Address
  - Configure NAT for internal servers
  - Configure P334WT behind a NAT router
  - Relaying NetBIOS Broadcast over IPSec tunnel

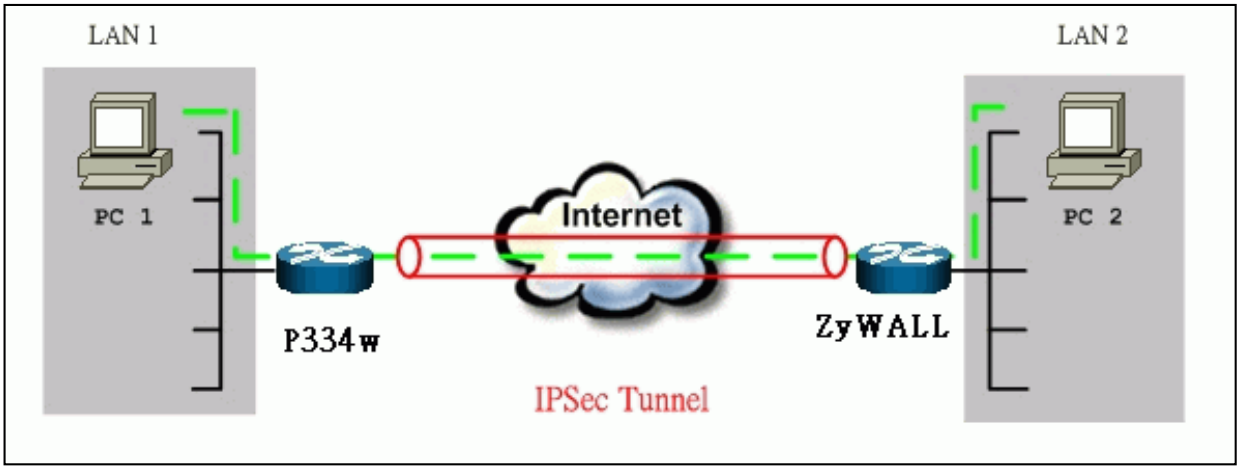
P334WT to ZyWALL Tunneling

1. Setup P334WT
2. Setup ZyWALL
3. Troubleshooting
4. View Log

This page guides us to setup a VPN connection between P334WT and ZyWALL router. Please note that, in addition to P334w to ZyWALL, P334WT can also talk to other VPN hardwards. The tested VPN hardware are shown below.

- 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 ZyWALL
- Avaya VPN
- Netopia VPN
- III VPN

As the figure shown below, the tunnel between P334WT and ZyWALL ensures the packets flow between PC 1 and PC 2 are secure. Because the packets go through the IPSec tunnel are encrypted. To achieve this VPN tunnel, the settings required for each P334WT and ZyWALL are explained in the following sections.



The IP addresses we use in this example are as shown below.

PC 1	P334WT	ZyWALL	LAN 2
192.168.1.33	LAN: 192.168.1.1 WAN: 202.132.154.1	LAN: 192.168.2.1 WAN: 168.10.10.66	192.168.2.0/24

Note:

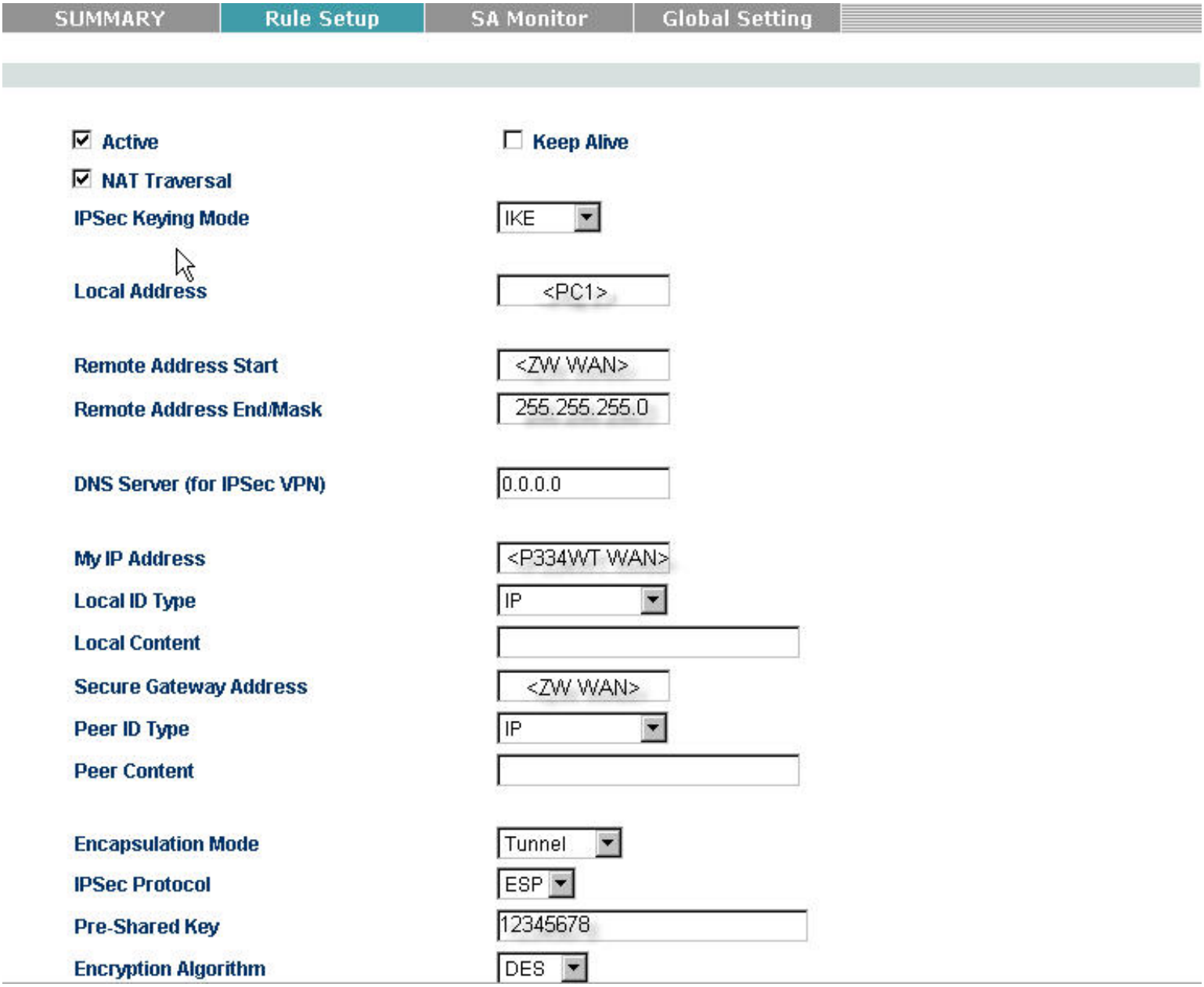
1. The following configurations are supposed both two VPN gateways have fixed IP addresses. If one of VPN gateways uses dynamic IP, we enter **0.0.0.0** as the secure gateway IP address. In this case, the VPN connection can only be initiated from dynamic side to fixed side to update its dynamic IP to the fixed side. However, if both gateways use dynamic IP addresses, it is no way to establish VPN connection at all.
2. In this example, we presume that P334WT's model name is P334WT. And since it's P334WT, so only 1 PC can use the tunnel.
3. In this example, we presume that ZyWALL's model name is ZyWALL10W.

---

1. Setup P334WT

1. Using a web browser, login P334WT by giving the LAN IP address of P334WT in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.
2. Click **Advanced**, and click **VPN** tab on the left.
3. On the **SUMMARY** menu, Select a policy to edit by clicking **Edit**.
4. On the **Rule-Setup** menu, check **Active** check box and give a name to this policy.
5. Local Address is PC1's IP address.
6. Remote Address Start is
7. **Destination IP Address Start** and **Destination IP Address End** are **PC 2** IP in this example. (the secure remote host)
8. **My IP Addr** is the **WAN IP of P334WT.**
9. **Secure Gateway IP Addr** is the remote secure gateway IP, that is **ZyWALL WAN IP** in this example.
10. Select **Encapsulation Mode** to **Tunnel**.
11. Check the **ESP** check box. (AH can not be used in SUA/NAT case)
12. Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **MD5**, as we configured in ZyWALL.
13. Enter the key string **12345678** in the **Preshared Key** text box, and click **Apply**.

See the screen shot:

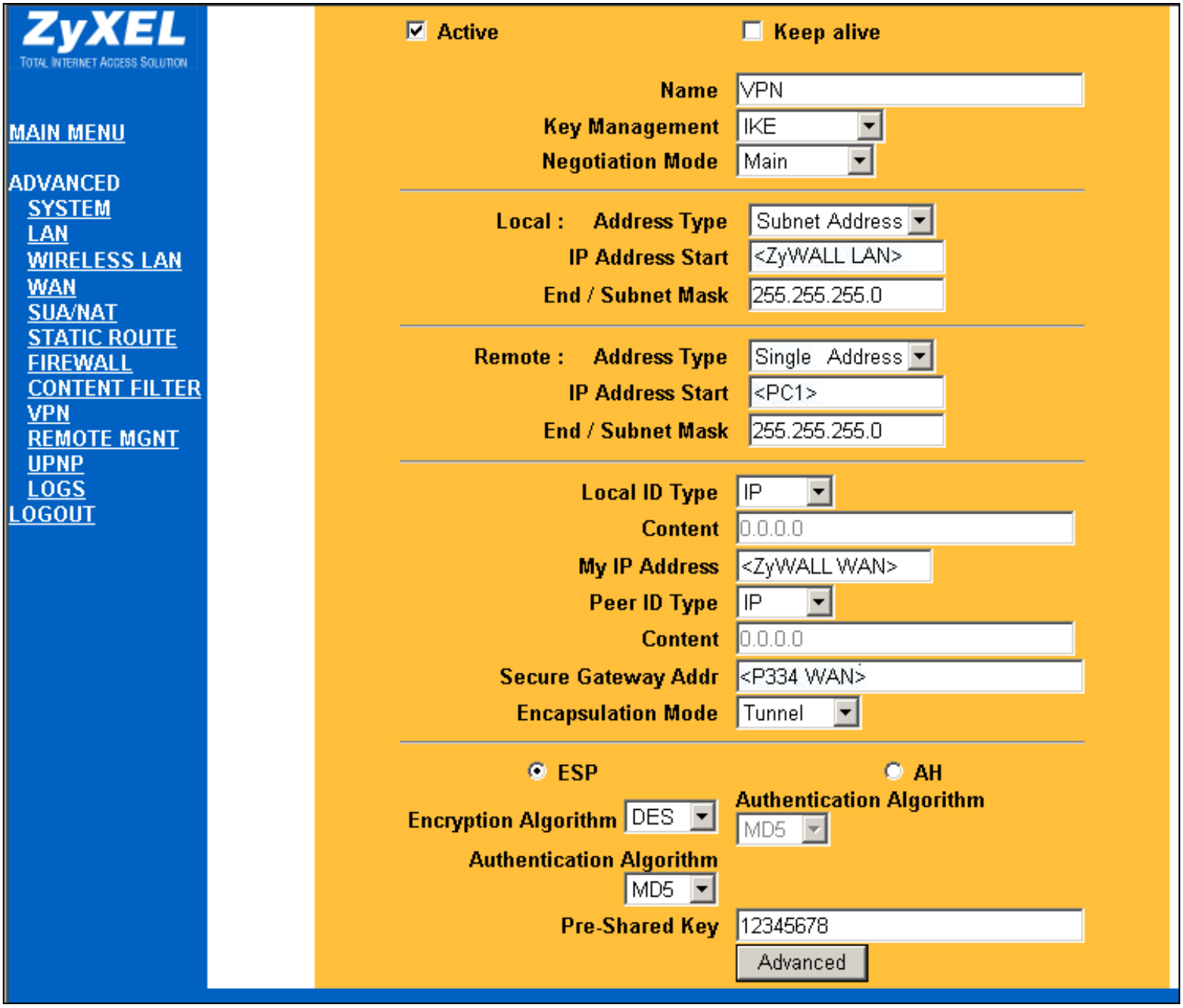


2. Setup ZyWALL

Similar to the settings for P334WT, ZyWALL is configured in the same way.

1. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field.
2. Click **Advanced**, and click **VPN** tab on the left.
3. On the **SUMMARY** menu, Select a policy to edit by clicking **Edit**.
4. On the **CONFIGURE-IKE** menu, check **Active** check box and give a name to this policy.
5. Select **IPSec Keying Mode** to **IKE** and **Negotiation Mode** to **Main**, as we configured in P334WT.
6. **Source IP Address Start** and **Source IP Address End** are **PC 2** IP in this example. (the secure host behind ZyWALL)
7. **Destination IP Address Start** and **Destination IP Address End** are **PC 1** IP in this example. (the secure remote host)
   Note: You may assign a range of Local/Remote IP addresses for multiple VPN sessions**.**
8. **My IP Addr** is the **WAN IP of ZyWALL.**
9. **Secure Gateway IP Addr** is the remote secure gateway IP, that is **P334WT's WAN IP** in this example.
10. Select **Encapsulation Mode** to **Tunnel**.
11. Check the **ESP** check box. (AH can not be used in SUA/NAT case)
12. Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **MD5**, as we configured in **P334WT**.
13. Enter the key string **12345678** in the **Preshared Key** text box, and click **Apply**.

See the screen shot:



---

3. Troubleshooting

Q: How do we know the above tunnel works?

A: If the connection between PC 1 and PC 2 is ok, we know the tunnel works.

Please try to ping from PC 1 to PC 2 (or PC 2 to PC 1). If PC 1 and PC 2 can ping to each other, it means that the IPSec tunnel has been established successfully. If the ping fail, there are two methods to troubleshoot IPSec in P334WT.

- Menu 27.2, SA Monitor

Through menu 27.2, you can monitor every IPSec connections running in P334WT presently. The second column of each entry indicates the IPSec rule name. So, if you can't see the name of your IPSec rule, it means that the SA establishment fails. Please go back Menu 27 to check your settings.

```
                  Menu 27.2 - SA Monitor

 #                    Name                                Encap.  IPSec ALgorithm
 -- ------------------------------------------------- ----------
-------------------------
 1  ZyWALL      ca24f1eb6616b7c4 732c211ae9b01a0f   Tunnel   ESP DES-SHA1
 2
 3
 4
 5
 6
 7
 8
 9
 10

                    Select Command= Refresh
                    Select Connection= N/A

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

- Using CI command '**ipsec debug 1**'

Please enter '**ipsec debug 1**' in Menu 24.8. There should be lots of detailed messages printed out to show how negotiations are taken place. If IPSec connection fails, please dump 'ipsec debug 1' for our analysis. The following shows an example of dumped messages.

```
P334WT> ipsec debug 1
IPSEC debug level 1
P334WT> catcher(): recv pkt numPkt<1>
get_hdr nxt_payload<1> exchMode<2> m_id<0> len<80>
f76af206 b187aae3 00000000 00000000 01100200 00000000 00000050 00000034
00000001 00000001 00000028 01010001 00000020 01010000 80010001 80020001
80040001 80030001 800b0001 800c0e10
In isadb_get_entry, nxt_pyld=1, exch=2
New SA
In responder
isadb_create_entry(): RESPONSOR:
##entering spGetPeerByAddr...
<deleted>
```

4. View Log

To view the log for IPSec and IKE connections, please enter menu 27.3, View IPSec Log. The log menu is also useful for troubleshooting please capture to us if necessary. The example shown below is a successful IPSec connection.

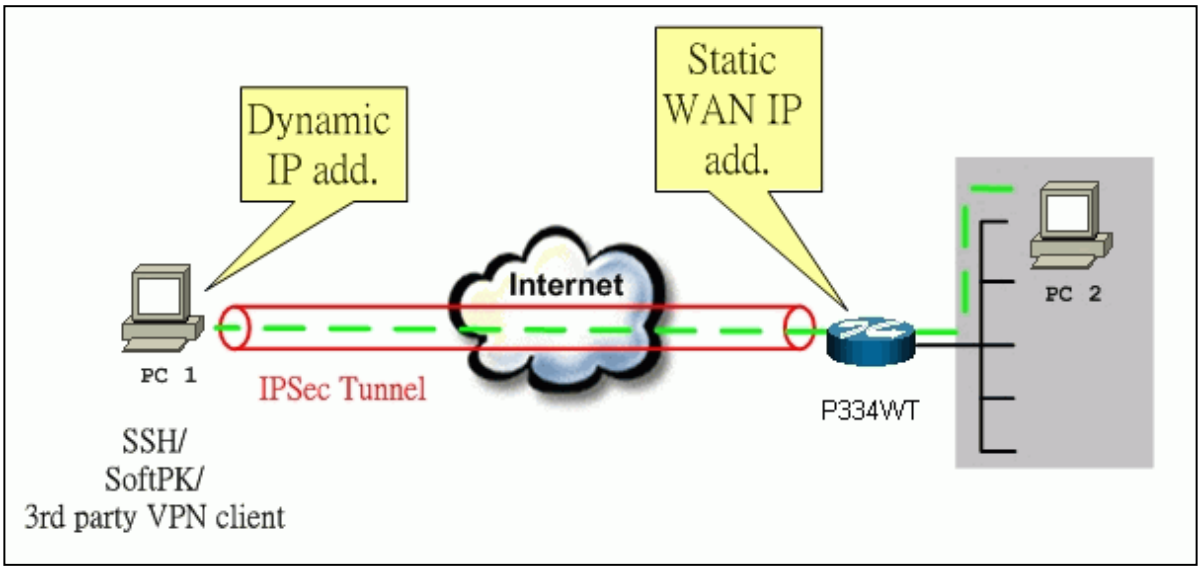
```
Index: Date/Time:         Log:
------------------------------------------------------------
001    01 Jan 10:23:22   !! Cannot find outbound SA for rule <1>
002    01 Jan 10:23:22   Send Main Mode request to <168.10.10.66>
003    01 Jan 10:23:22   Send:<SA>
004    01 Jan 10:23:22   Recv:<SA>
005    01 Jan 10:23:24   Send:<KE><NONCE>
006    01 Jan 10:23:24   Recv:<KE><NONCE>
007    01 Jan 10:23:26   Send:<ID><HASH>
008    01 Jan 10:23:26   Recv:<ID><HASH>
009    01 Jan 10:23:26   Phase 1 IKE SA process done
010    01 Jan 10:23:26   Start Phase 2: Quick Mode
011    01 Jan 10:23:26   Send:<HASH><SA><NONCE><ID><ID>
012    01 Jan 10:23:26   Recv:<HASH><SA><NONCE><ID><ID>
013    01 Jan 10:23:26   Send:<HASH>
Clear IPSec Log (y/n):
```

Secure Gateway with Dynamic WAN IP Address

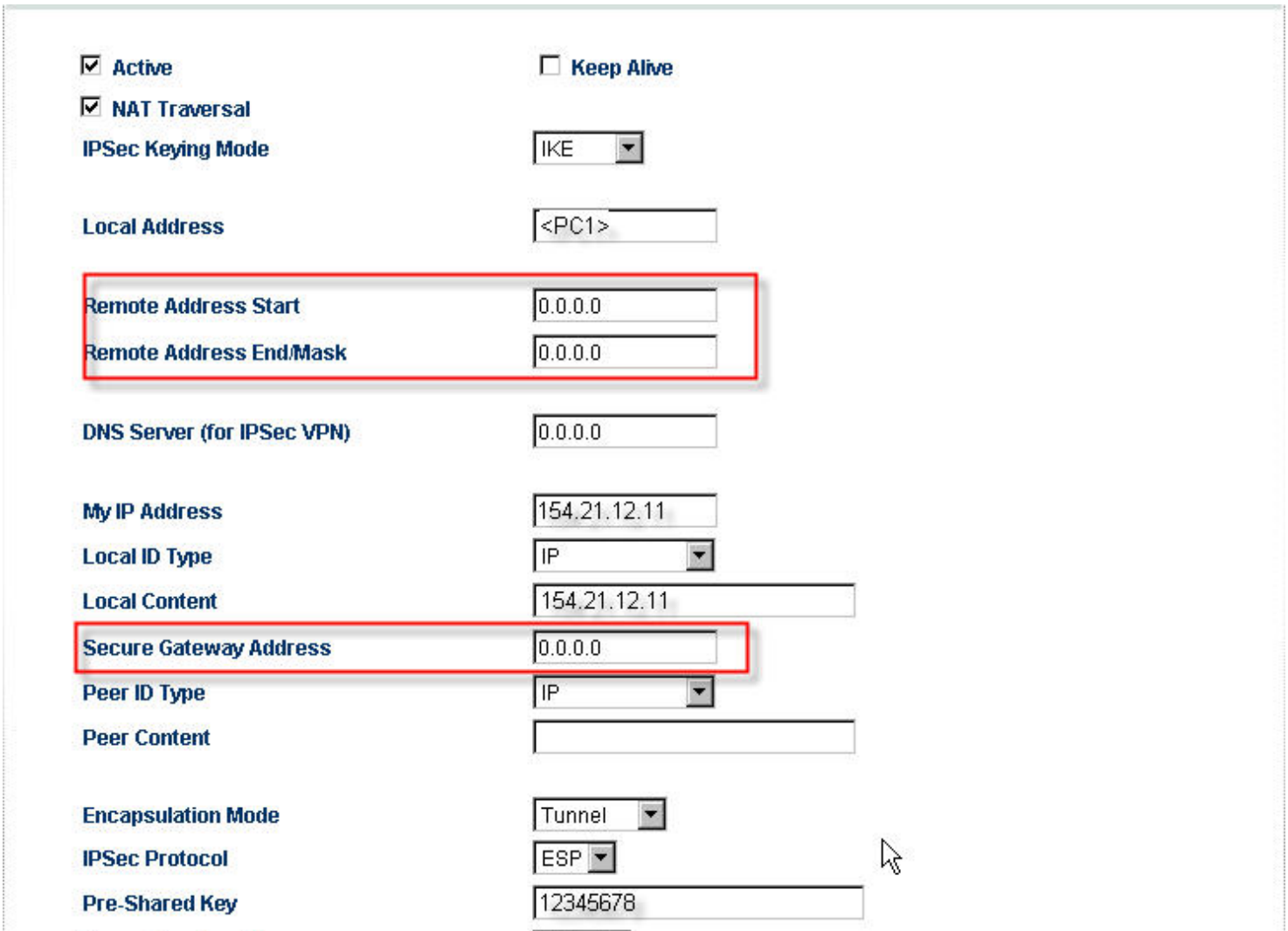
- P334WT static WAN IP v.s. peer side dynamic IP
- P334WT dynamic WAN IP v.s. peer side static IP

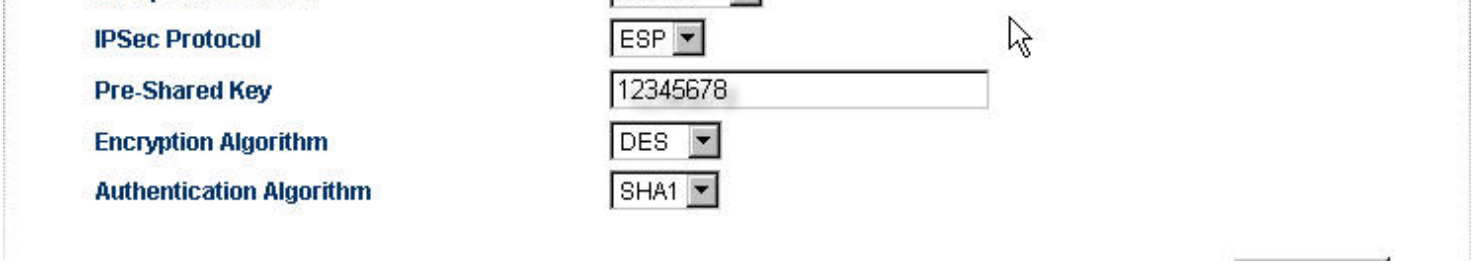
Most of the cases, static IP addresses are used for VPN tunneling endpoints. But for SOHO users, generally, it is a dynamic case. In this case, this IP will not be available to pre-defined in the VPN box. There are some tips when configuring ZyWALL in any dynamic case.

- **ZyWALL static WAN IP v.s. peer side dynamic IP**



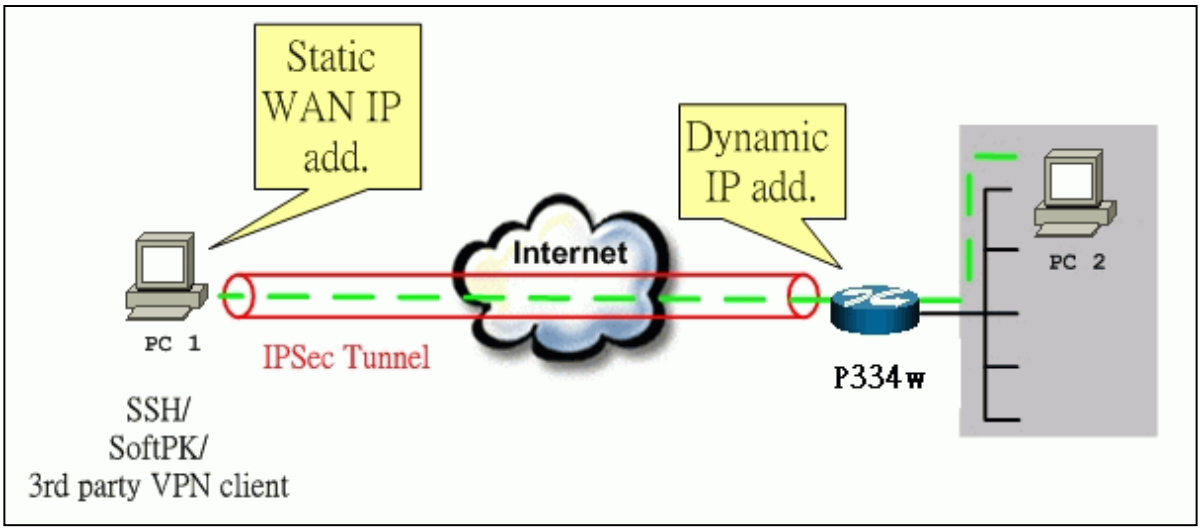
1. In VPN settings of P334WT, please specify the IP address of **Secure Gateway** as **0.0.0.0**.



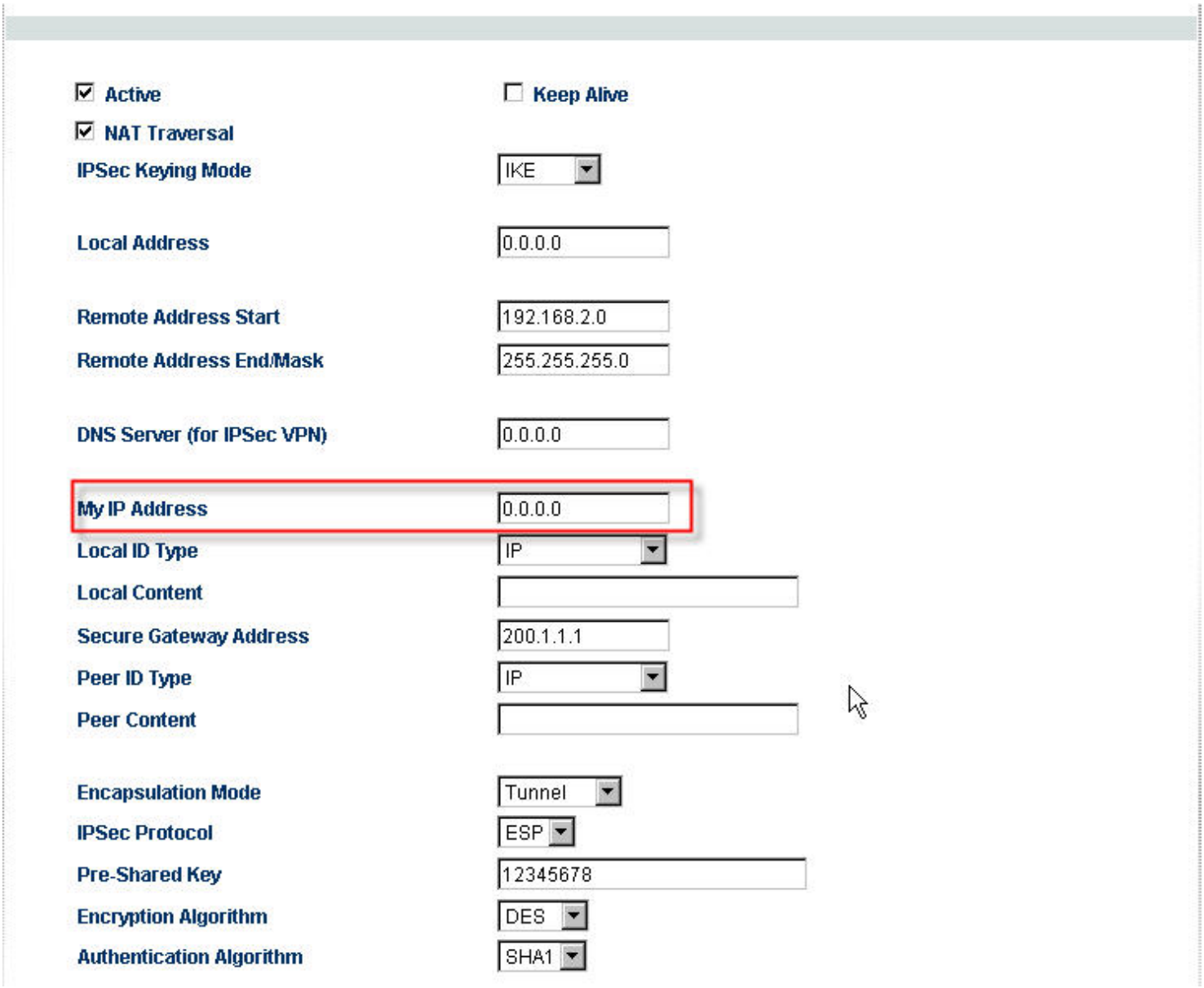


2. In remote side, generally speaking, most VPN clients will bind PPP/Ethernet adapter's dynamic IP address to IPSec automatically . The only thing you need to concern is to specify the interface you want to apply IPSec/VPN correctly. The rest parts are similar with that in static cases.
3. Afterward, the VPN connection can **ONLY** be initiated from dynamic side to static side in order to update its dynamic IP to the static side.
4. In peer side, Are you using **Win2K built-in IPSec**? In this case, W2K won't capture the dynamic IP address automatically for you. You have to obtain your dynamic IP address and then go back to IPSec configuration to setup your current IP address.

- **P334WT dynamic WAN IP v.s. peer side static IP**



1. In VPN settings of P334WT, please specify the IP address of **My IP** as **0.0.0.0**. P334WT will automatically bind it's current WAN IP address to IPSec.



2. IPSec tunnel in this case, can **ONLY** be initiated from P334WT.

Configure NAT for Internal Servers

Some tips for this application:

Generally, without IPSec, to configure an internal server for outside access, we need to configure the server private IP and its service port in SUA/NAT Server Table. The NAT router then will forward the incoming connections to the internal server according to the service port and private IP entered in SUA/NAT Server Table.

However, if both NAT and IPSec is enabled in P334WT, the edit of the table is necessary only if the connection is a non-secure connections. For secure connections, none SUA server settings are required since private IP is reachable in the VPN case. Remember, IPSec is an IP-in-IP encapsulation, the internal IP header is not translated by NAT.

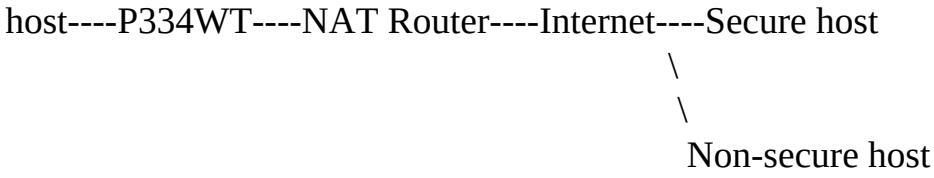
For example:

Internal Server----P334WT(NAT+IPSec)-----ADSL Modem----Internet----Remote Network

Configure P334w Behind a NAT Router

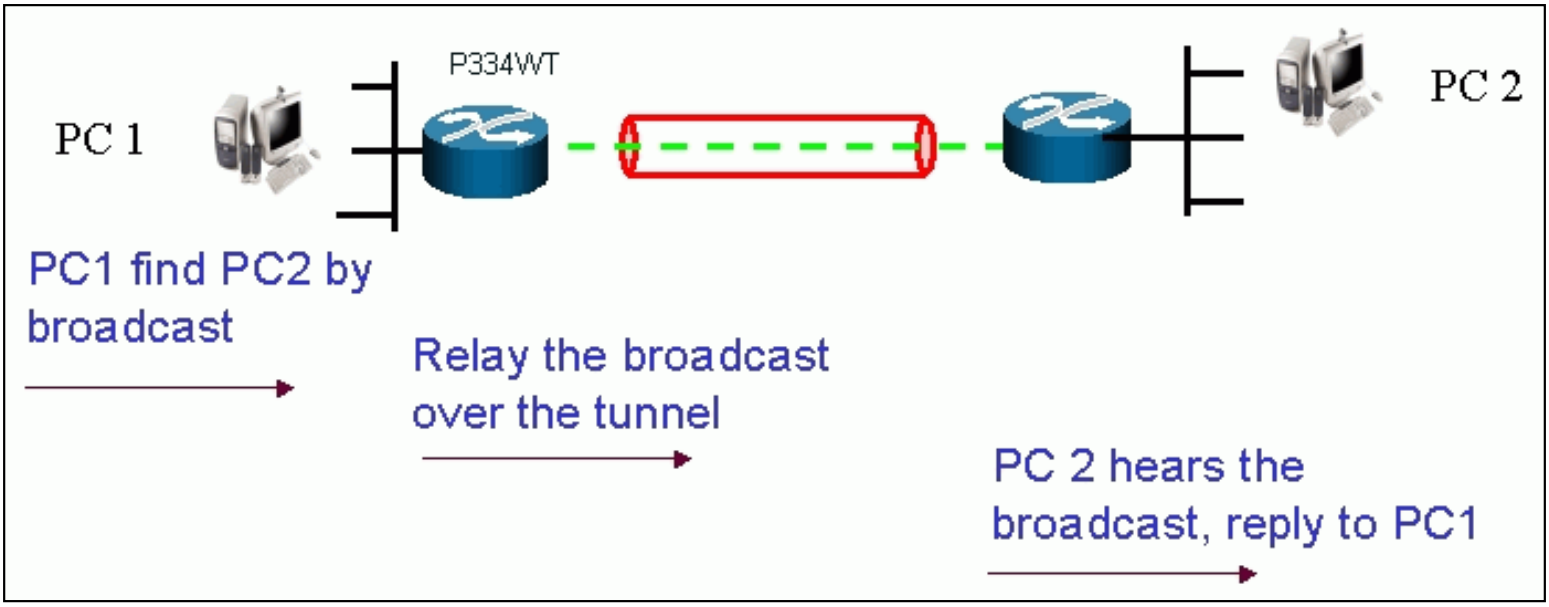
Some tips for this application:

1. The NAT router must support to pass through IPSec protocol. Only ESP tunnel mode is possible to work in NAT case. If the NAT router is ZyXEL NAT router (P300 series, P643, P642, or P202) supporting IPSec pass through, default port and the P334w WAN IP must be configured in their SUA/NAT Server Table.
2. WAN IP of the NAT router is the tunneling endpoint for this case, not the WAN IP of P334WT.
3. If firewall is turned on in P334WT, you must forward **IKE** port in Internet interface.
4. If NAT are also enabled in P334WT, NAT server is required for non-secure connections, NAT server is not required for secure connections and the phyical private IP is used.



Relaying NetBIOS Broadcast over IPSec tunnel.

¡@



By NetBIOS broadcast supported in VPN tunnel, users of Microsoft Windows can search computers in remote VPN network by **"Computer Name"**. Users don¡¦t need to pre-edit lmhosts in his/her local computer nor setup WINS server in between.

```
ras> ipsec load 1
ras> ipsec disp
---------- IPSec Setup ----------
Index #= 1 Active= Yes KeepAlive= No Protocol= 0
Name= 1
My IP Addr= 0.0.0.0
Local ID Type = IP Addr
Peer ID Type = IP Addr
Local ID Content = 0.0.0.0
Peer ID Content = 0.0.0.0
Secure Gateway Addr= 0.0.0.0
Local: Addr Type= SINGLE
IP Addr Start= 192.168.1.33 End= N/A
Port Start= 0 End= N/A
Remote: Addr Type= N/A
IP Addr Start= N/A End= N/A
Port Start= N/A End= N/A
Enable Replay Detection= No Key Management= IKE
---------- IKE Setup ----------
Phase 1 - Negotiation Mode= Main
Pre-Shared Key= 12345678
Encryption Algorithm= DES Authentication Algorithm= MD5
SA Life Time (Seconds)= 28800
Key Group= DH1
Phase 2 - Active Protocol= ESP
Encryption Algorithm= DES Authentication Algorithm= MD5
SA Life Time (Seconds)= 28800
Encapsulation= Tunnel
Perfect Forward Secrecy (PFS)= None
```

---------- NetBios Setup ----------
Broadcast Pass Through /*<------broadcast is not turned on yet.*/
Status: Inactive
Group: none
ras> ipesc disp
Valid commands are:
sys exit ether ip
ipsec cnm
ras> ipsec config netbios active on
ras> ipsec save
ras> ipsec load 1
ras> ipsec disp
---------- IPSec Setup ----------
Index #= 1 Active= Yes KeepAlive= No Protocol= 0
Name= 1
My IP Addr= 0.0.0.0
Local ID Type = IP Addr
Peer ID Type = IP Addr
Local ID Content = 0.0.0.0
Peer ID Content = 0.0.0.0
Secure Gateway Addr= 0.0.0.0
Local: Addr Type= SINGLE
IP Addr Start= 192.168.1.33 End= N/A
Port Start= 0 End= N/A
Remote: Addr Type= N/A
IP Addr Start= N/A End= N/A
Port Start= N/A End= N/A
Enable Replay Detection= No Key Management= IKE
---------- IKE Setup ----------
Phase 1 - Negotiation Mode= Main
Pre-Shared Key= 12345678
Encryption Algorithm= DES Authentication Algorithm= MD5
SA Life Time (Seconds)= 28800
Key Group= DH1
Phase 2 - Active Protocol= ESP
Encryption Algorithm= DES Authentication Algorithm= MD5
SA Life Time (Seconds)= 28800
Encapsulation= Tunnel
Perfect Forward Secrecy (PFS)= None
---------- NetBios Setup ----------
Broadcast Pass Through /*<------broadcast is turned on.*/
Status: Active
Group: none

Wireless Application Notes

- Infrastructure Mode
- Wireless MAC Address Filtering
- WEP Configurations
- IEEE 802.1x
- Site Survey

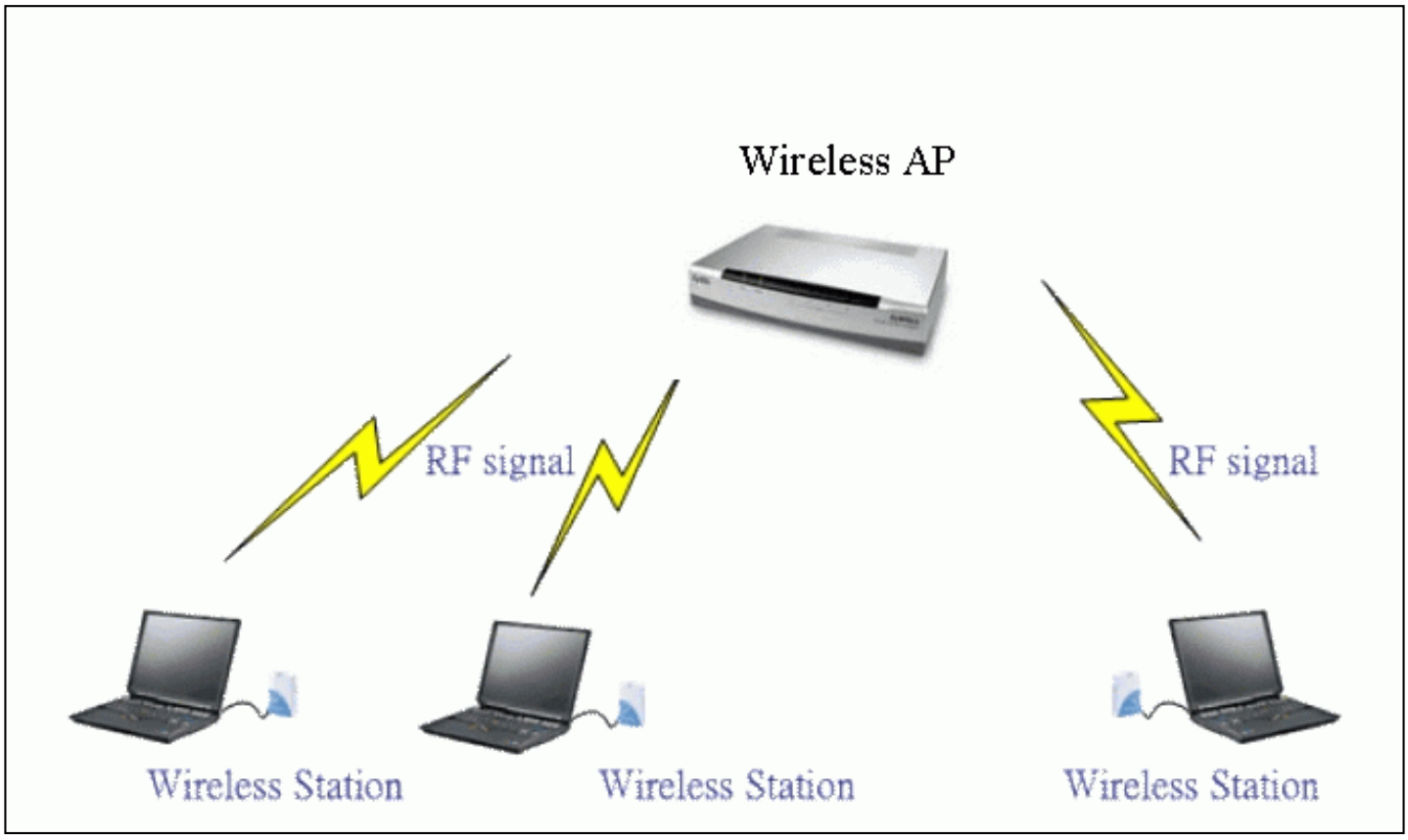
Configuring Infrastructure mode

¡@

- ***Introduction***

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 Wireless Access Point to Infrastructure mode using SMT.

To configure Infrastructure mode of your P334WT wireless AP please follow the steps below.

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

2. Enter 5 to display Menu 3.5 ¡V Wireless LAN Setup.

Menu 3.5 - Wireless LAN Setup

ESSID= ZyXEL
Hide ESSID= No
Channel ID= CH01 2412MHz
RTS Threshold= 4096
Frag. Threshold= 4096
WEP Encryption= N/A
Default Key= N/A
Key1= N/A
Key2= N/A
Key3= N/A
Key4= N/A
Authen. Method= N/A

Edit MAC Address Filter= No
Edit Roaming Configuration= No

Preamble= Long
802.11Mode= Mixed

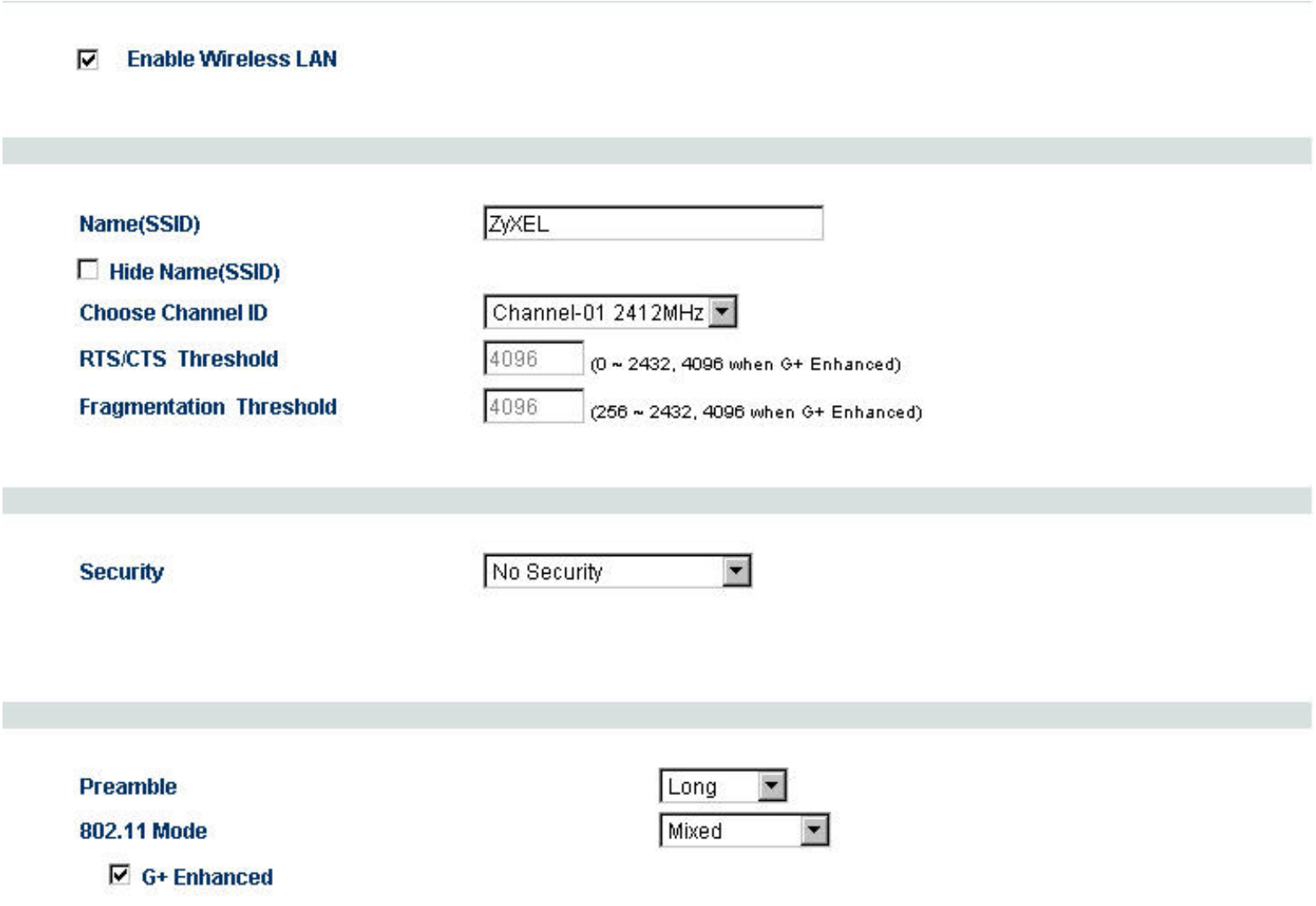
¡@

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

Configuration Wireless Access Point to Infrastructure mode using Web configurator.

To configure Infrastructure mode of your P334WT please follow the steps below.

1. From the web configurator main menu, go to Main Menu/Wireless LAN/Wireless.



3. Configure the desired configuation on P334WT.

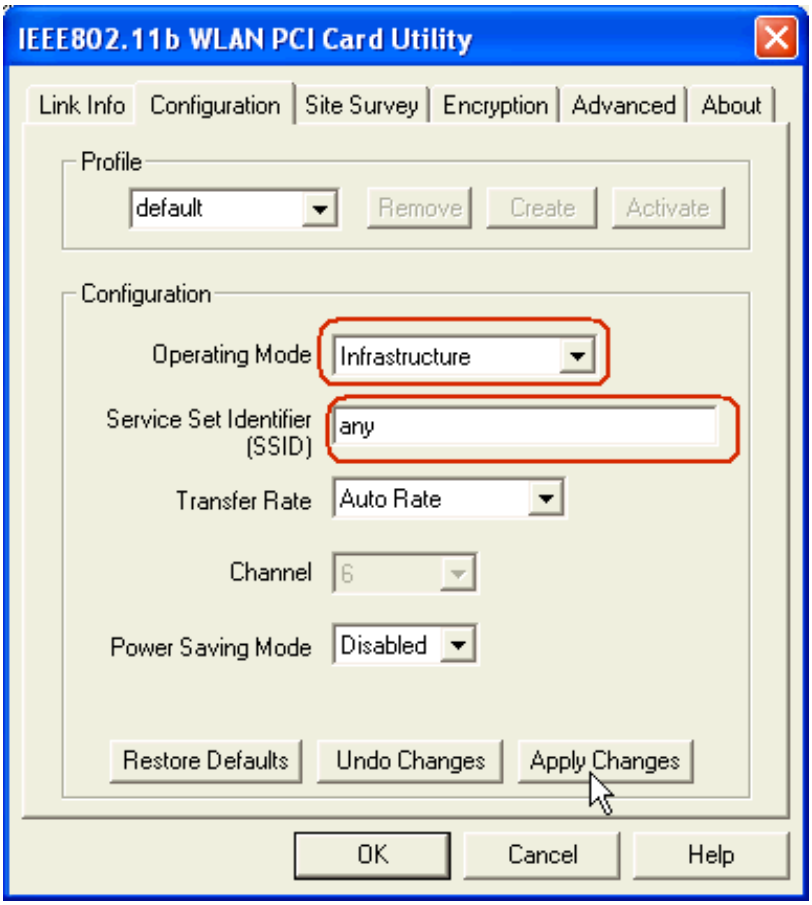
4. Finished.

- ***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.

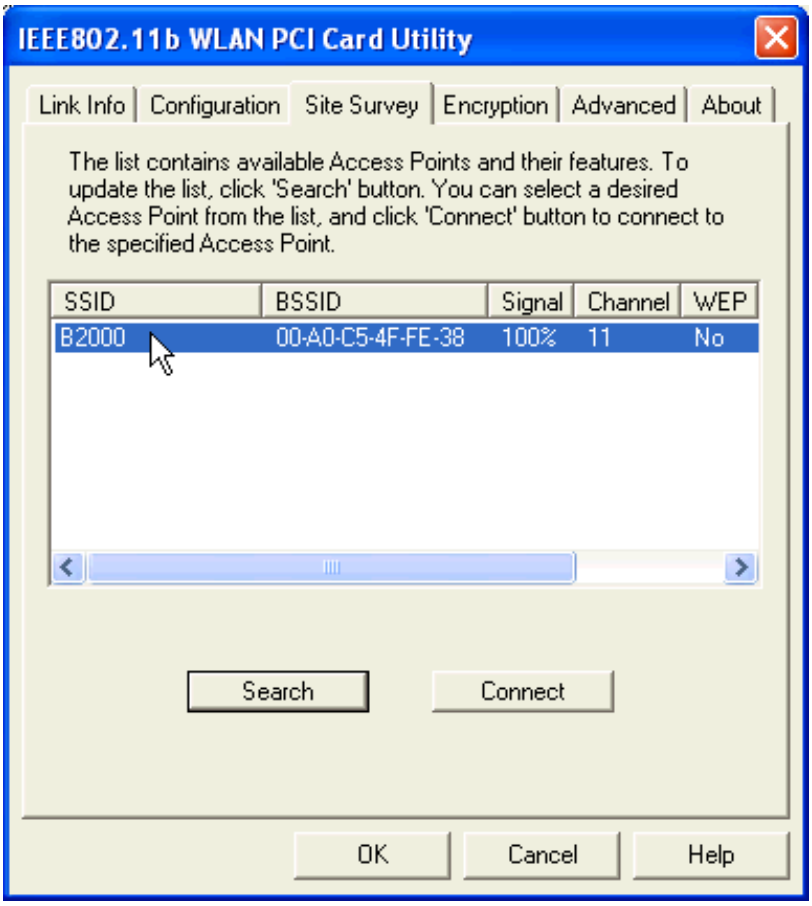
1. Double click on the utility icon in your windows task bar the utility will pop up on your windows screen.

2. Select configuration tab.

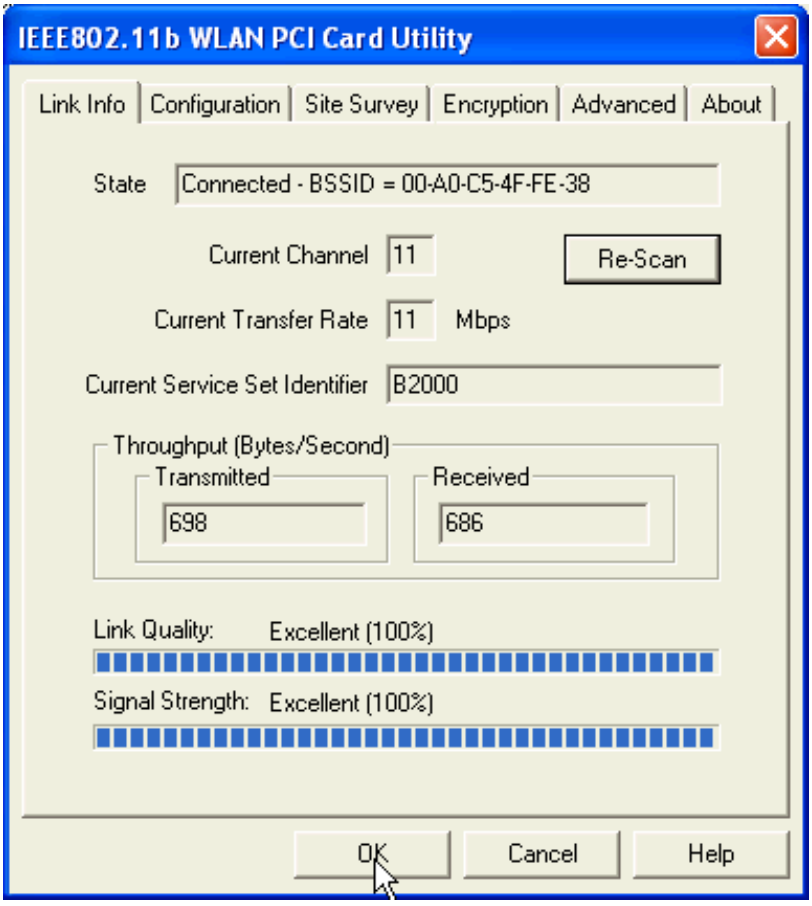


3. Select Infrastructure from the operation mode pull down menu, fill in an SSID or leave it as any if you wish to connect to any AP than press Apply Change to take effect.

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.



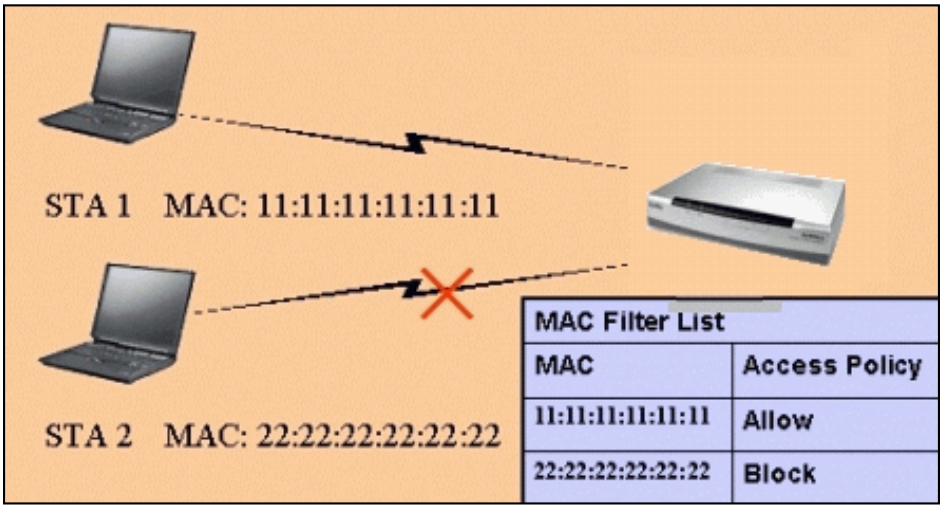
6. After the client have associated with the selected AP. The linked AP's channel, current linkup rate, SSID, link quality, and signal strength will show on the Link Info page. You now successfully associate with the selected AP with Infrastructure Mode.

MAC Filter

---

1. 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= No
Filter Action= Allowed Association
------------------------------------------------------------------------------
1= 00:00:00:00:00:00 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
Filter Action	Allow or block association from MAC addresses contained in this list. If **Allow Association** is selected in this field, hosts with MAC addresses configured in this list will be allowed to associate with AP. If **Deny Association** 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. go to Main Menu/Wireless LAN/MAC Filter and select **Yes** in the **Active** field to enable MAC Filter.
3. Select the **Filter Action** to allow or deny association from hosts in the list.
4. Enter the MAC Addresses which you may want to apply the filter to allow or block associations from.
5. Click **Apply** to make your setting work.

MAC Address Filter

Active Yes

Filter Action Allow Association

Set	MAC Address	Set	MAC Address
1	00:a0:c5:11:22:33	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00

Setup WEP (Wired Equivalent Privacy)

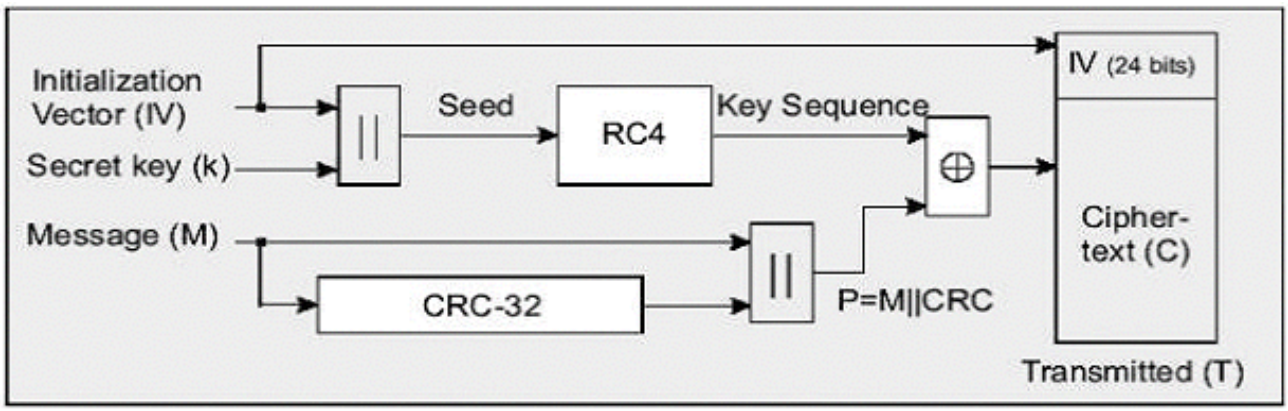
Introduction

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

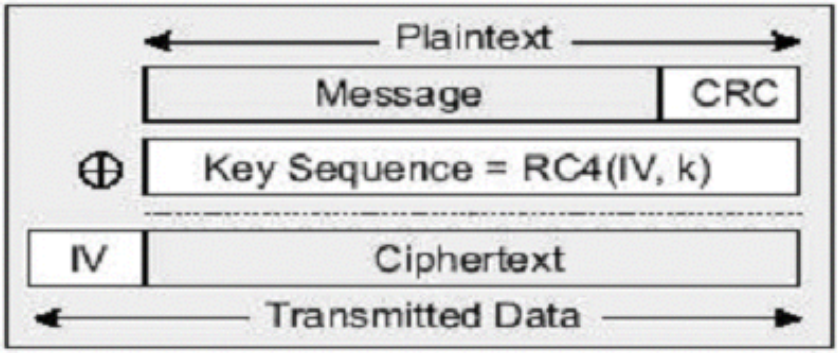
The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping, because wireless transmissions are easier to intercept than transmissions over wired networks, and wireless is a shared medium, everything that is transmitted or received over a wireless network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

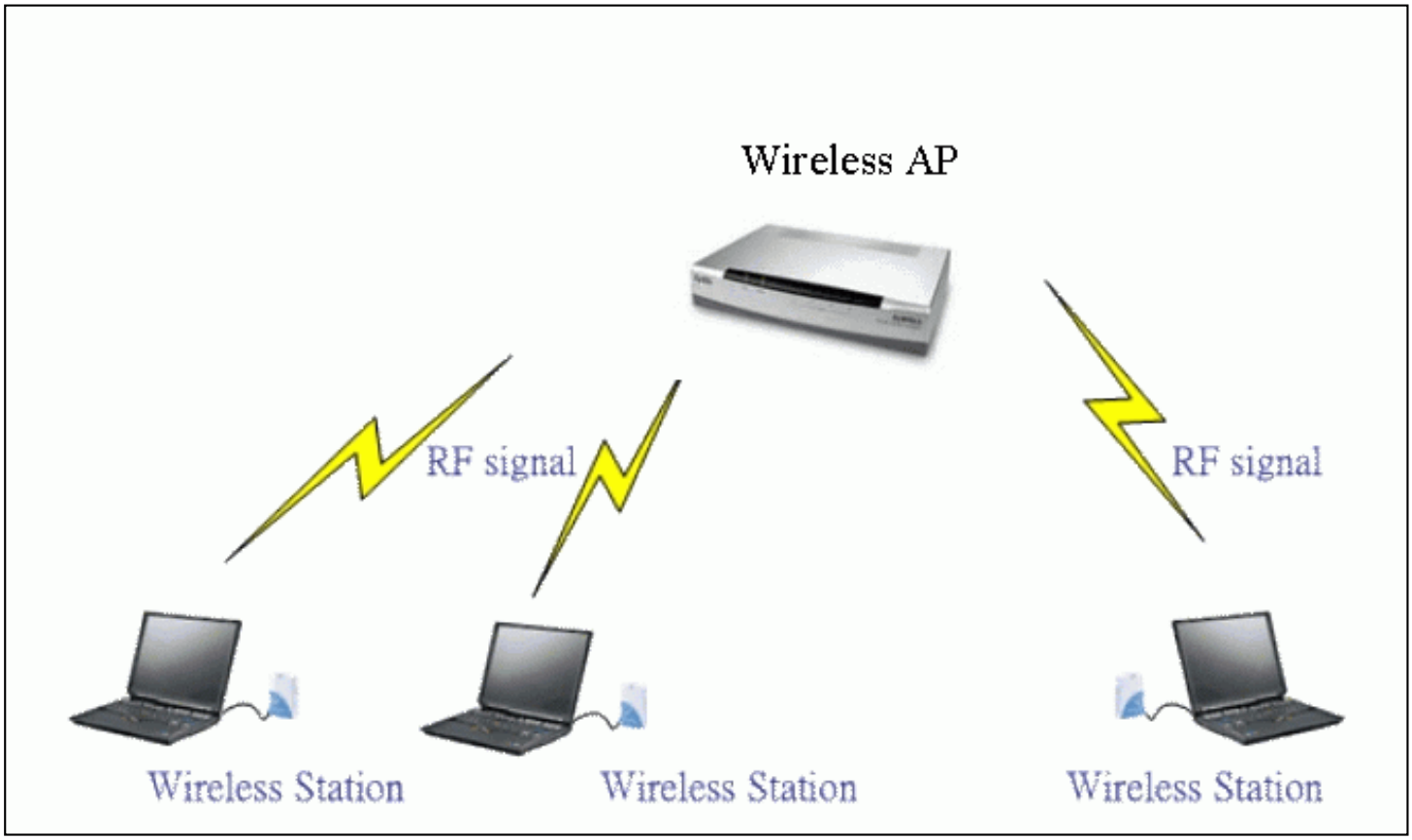
WEP employs the key encryption algorithm, Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG). The same key is used to encrypt and decrypt the data.



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 reson 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,

```
Menu 3.5 - Wireless LAN Setup

ESSID= B1000
Hide ESSID= No
Channel ID= CH01 2412MHz
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
Edit Roaming Configuration= 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= **0x**123456789A Key2= **0x**23456789AB Key3= **0x**3456789ABC Key4= **0x**456789ABCD
128-bit WEP with 13 characters	Key1= 2e3f4w345ytre Key2= 5y7jse8r4i038 Key3= 24fg70okx3fr7 Key4= 98jui2wss35u4
128-bit WEP with 26 hexadecimal digits ('0-9', 'A-F')	Key1= **0x**112233445566778899AABBCDEF Key2= **0x**2233445566778899AABBCCDDEE Key3= **0x**3344556677889900AABBCCDDFF Key4= **0x**44556677889900AABBCCDDEEFF

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.

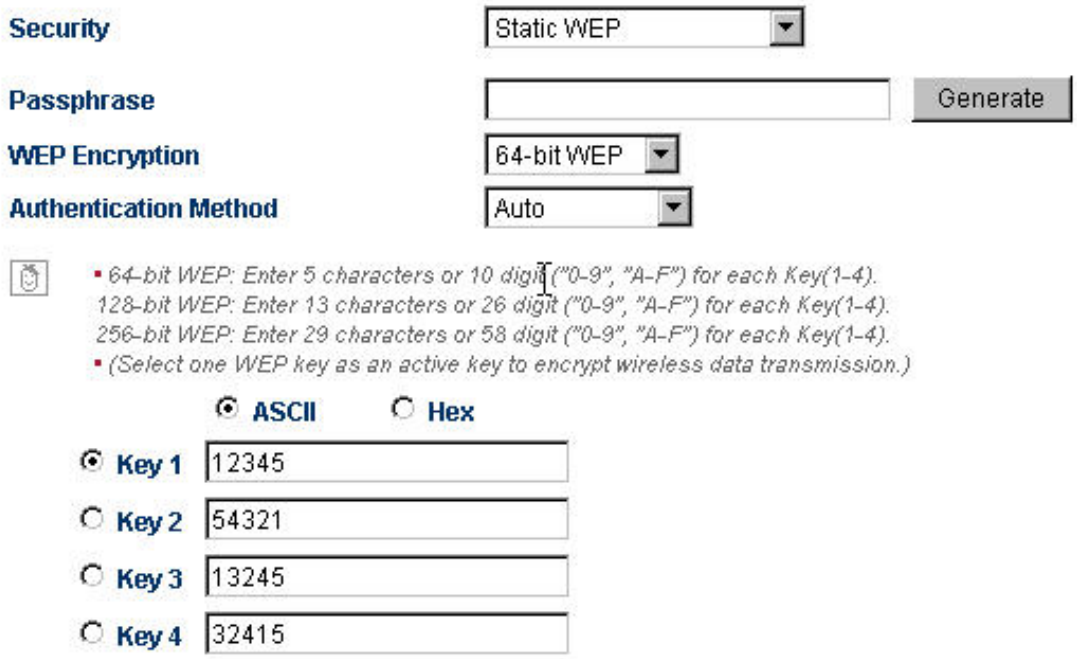
Access Point (encrypt data by Key 3) --------> Station (decrypt data by Key 3)

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



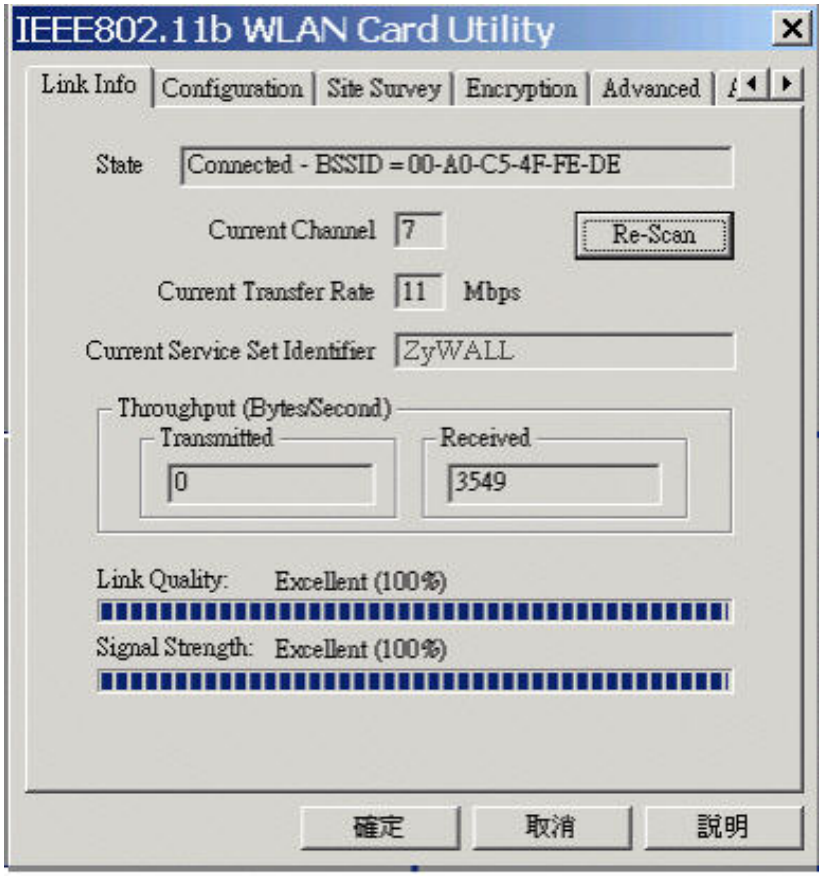
Key settings

Select one WEP key as default key to encrypt wireless data transmission.

Setting up the Station

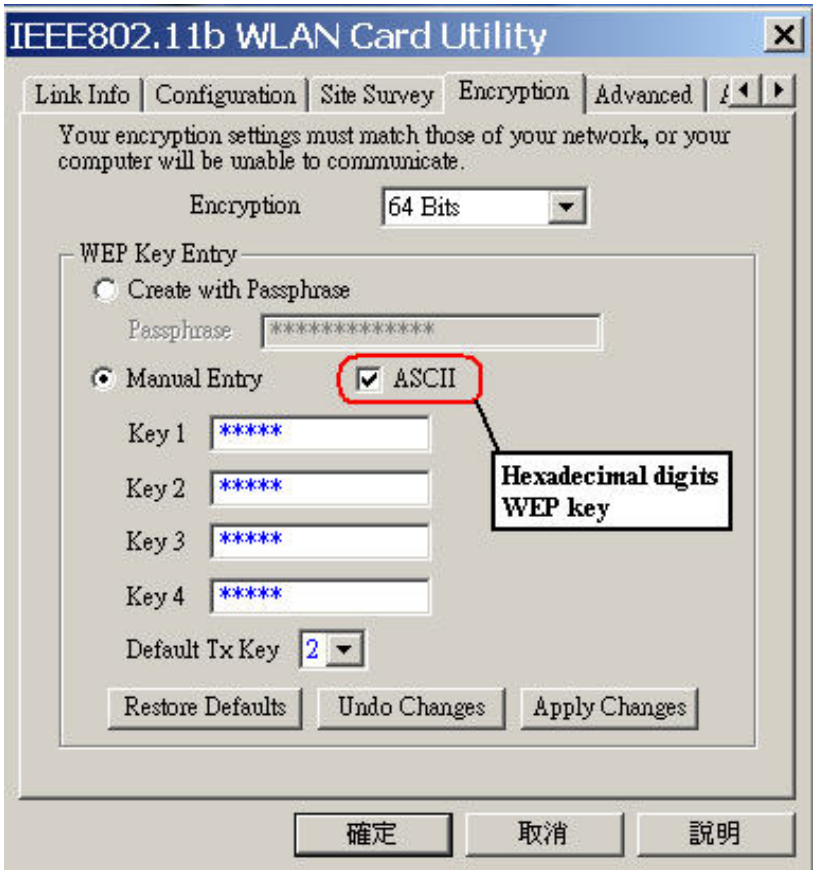
1. Double click on the utility icon in your windows task bar or right click the utility icon then select 'Show Config Utility'.

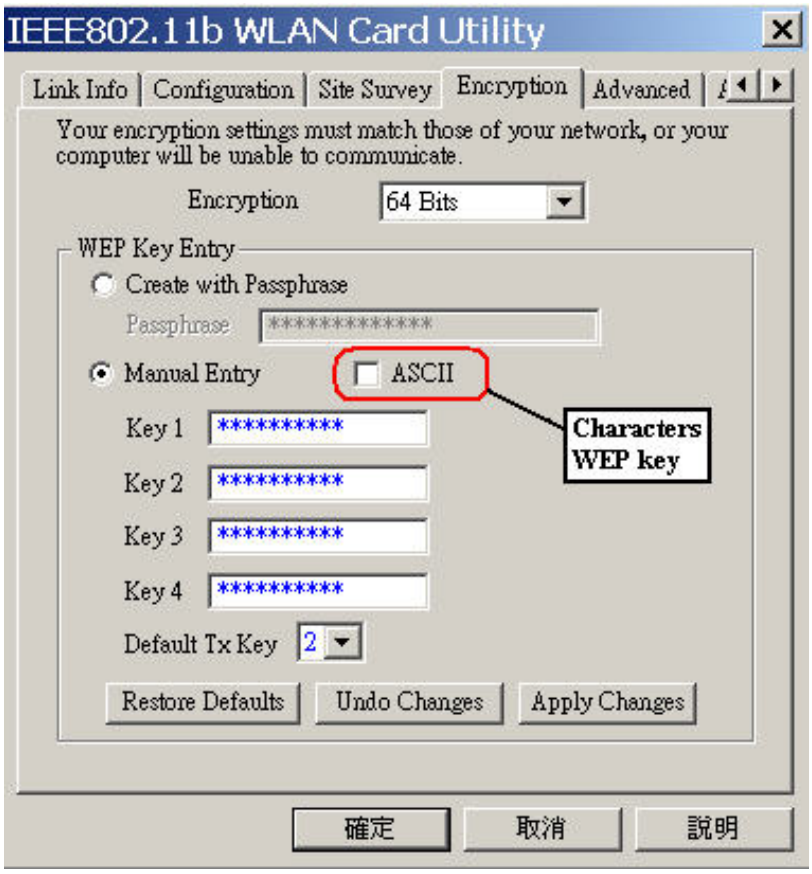
The utility will pop up on your windows screen.



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 preceded by '0x'.
For example,

64-bits with characters WEP key :
Key1= 2e3f4

Key2= 5y7js
Key3= 24fg7
Key4= 98jui

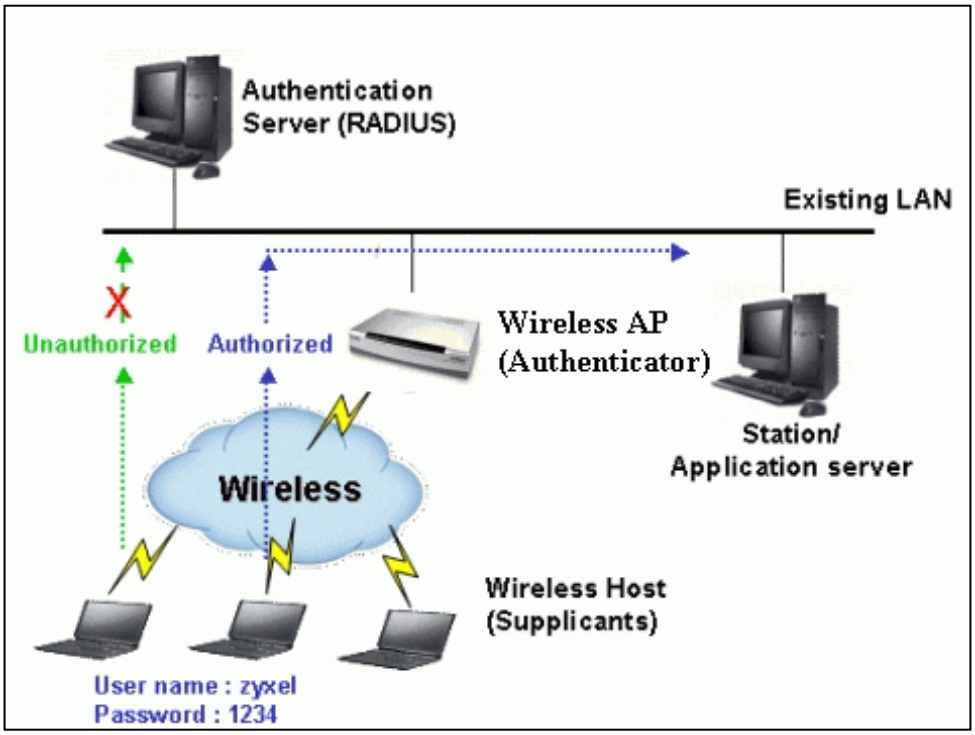
64-bits with hexadecimal digits WEP key :
Key1= 123456789A
Key2= 23456789AB
Key3= 3456789ABC
Key4= 456789ABCD

Setup IEEE 802.1x Access Control (Authentication and Accounting)

- What is IEEE 802.1x ?
    - IEEE 802.1x Introduction
    - Authentication Port State and Authentication Control
    - Re-Authentication
    - EAPOL
- Setup 802.1x in Wireless Access Point
    - Enable 802.1x
    - Using Internal Authentication Server
    - Using External RADIUS Authentication Server
- Setup 802.1x client in the Station

- ***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 tree 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.

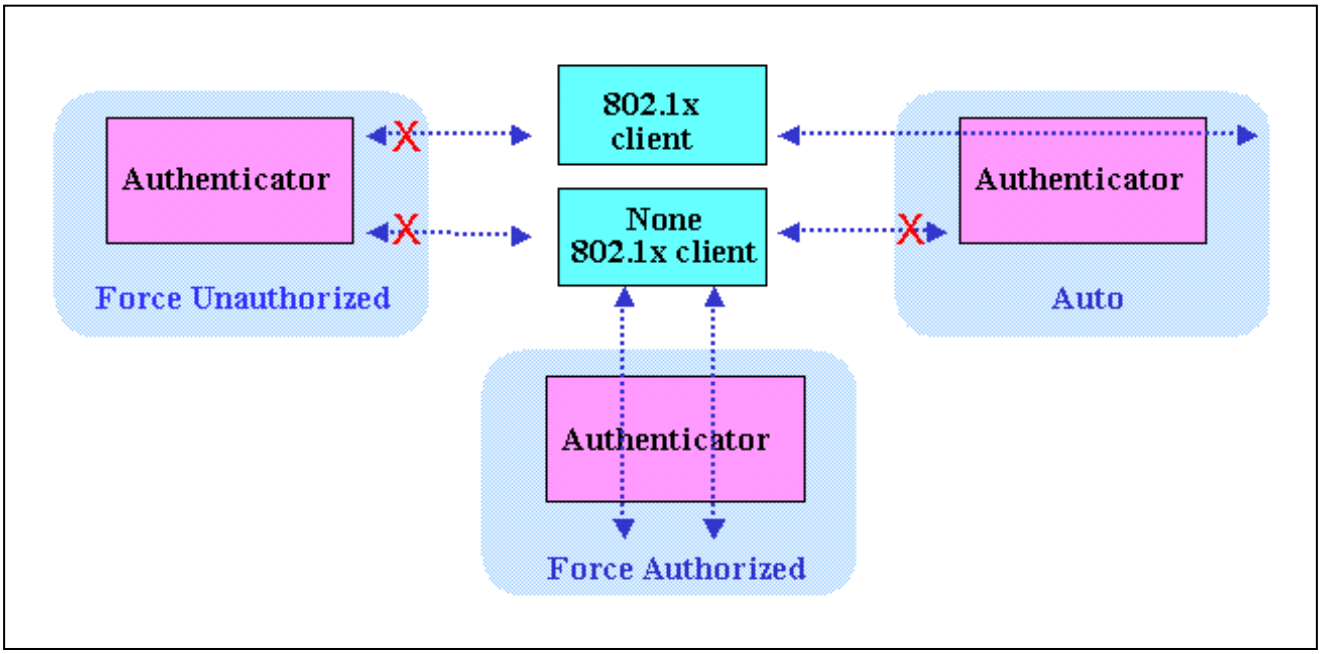
Some Wireless AP (i.e. ZyXEL Wireless AP) have built-in authentication server, external RADIUS authentication server is not needed. In this case, Wireless AP is acted as both authenticator and authentication server.

- ***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

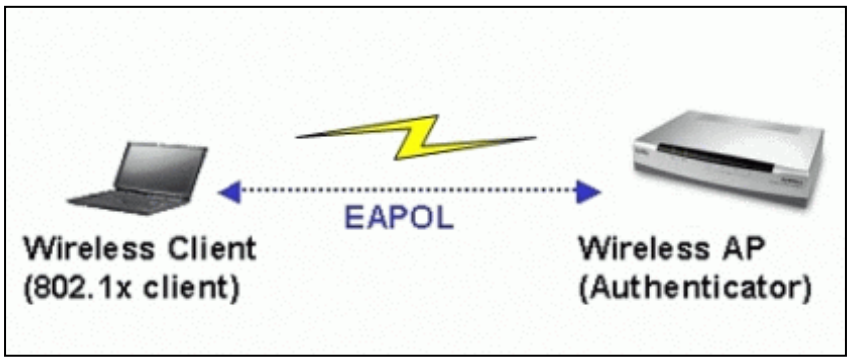
through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received requests the identity of the client and begins relaying authentication messages between supplicant and the authentication server. Each supplicant attempting 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.

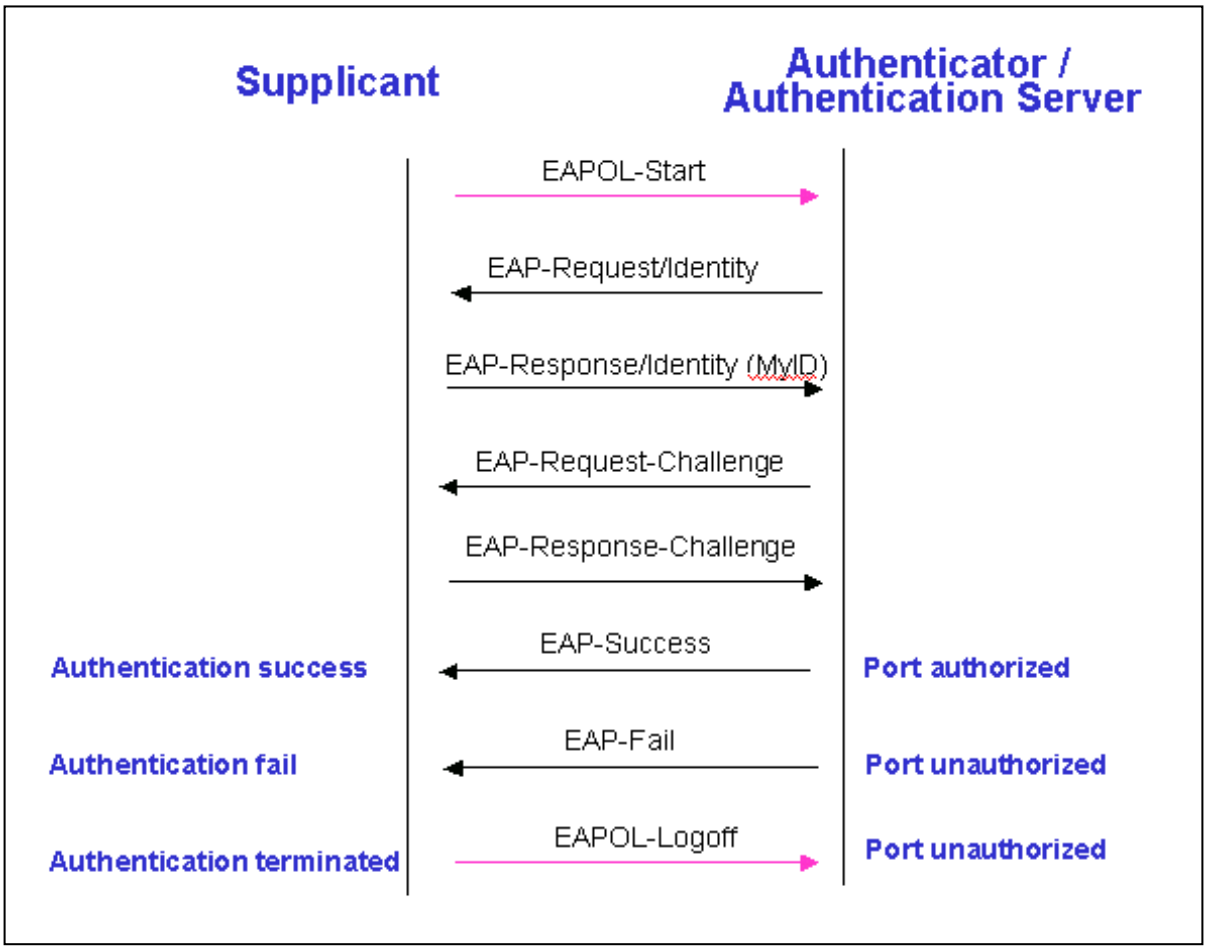


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When supplicant receive 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.

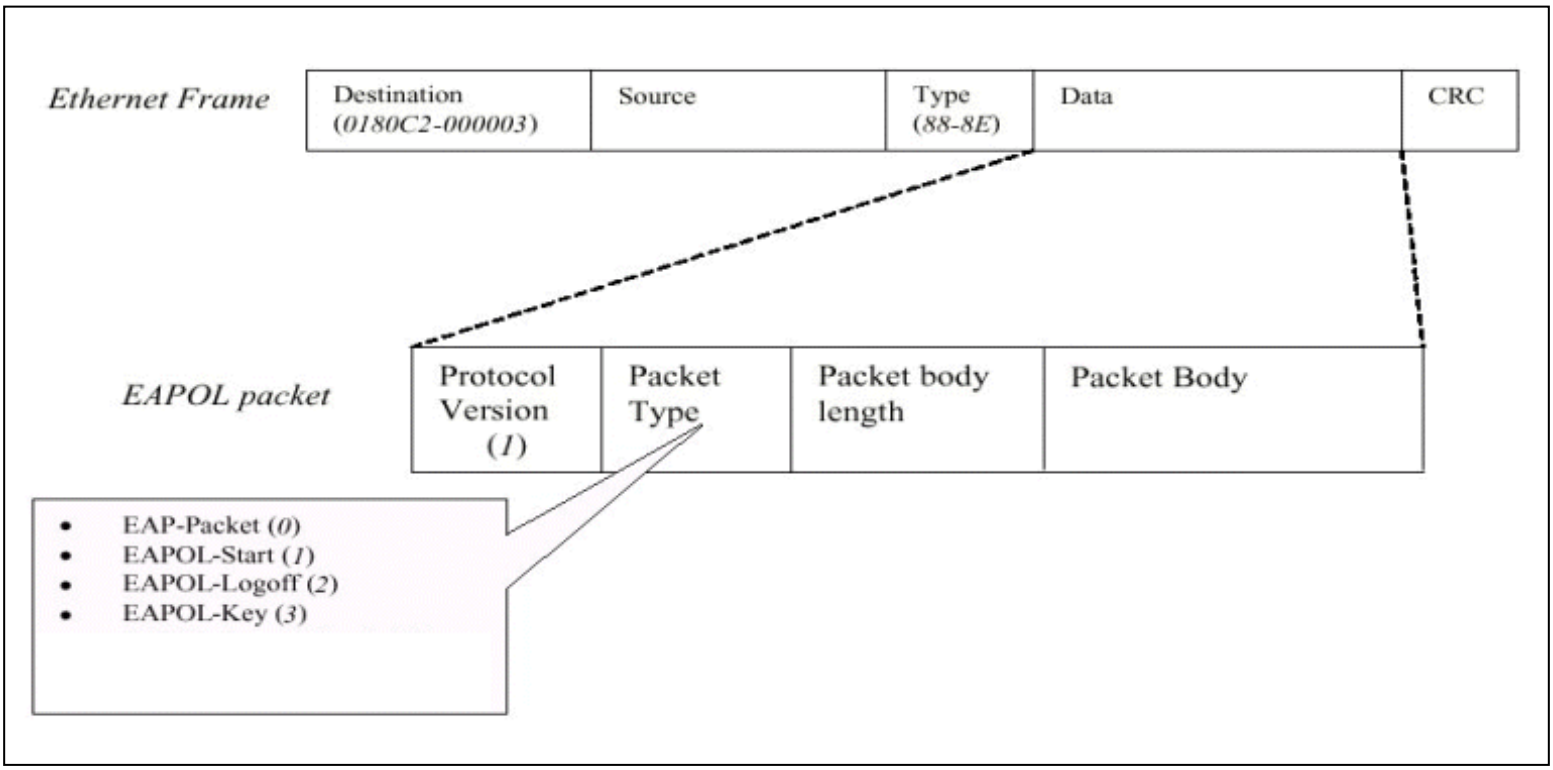
EAPOL Exchange between 802.1x Authenticator and Supplicant

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

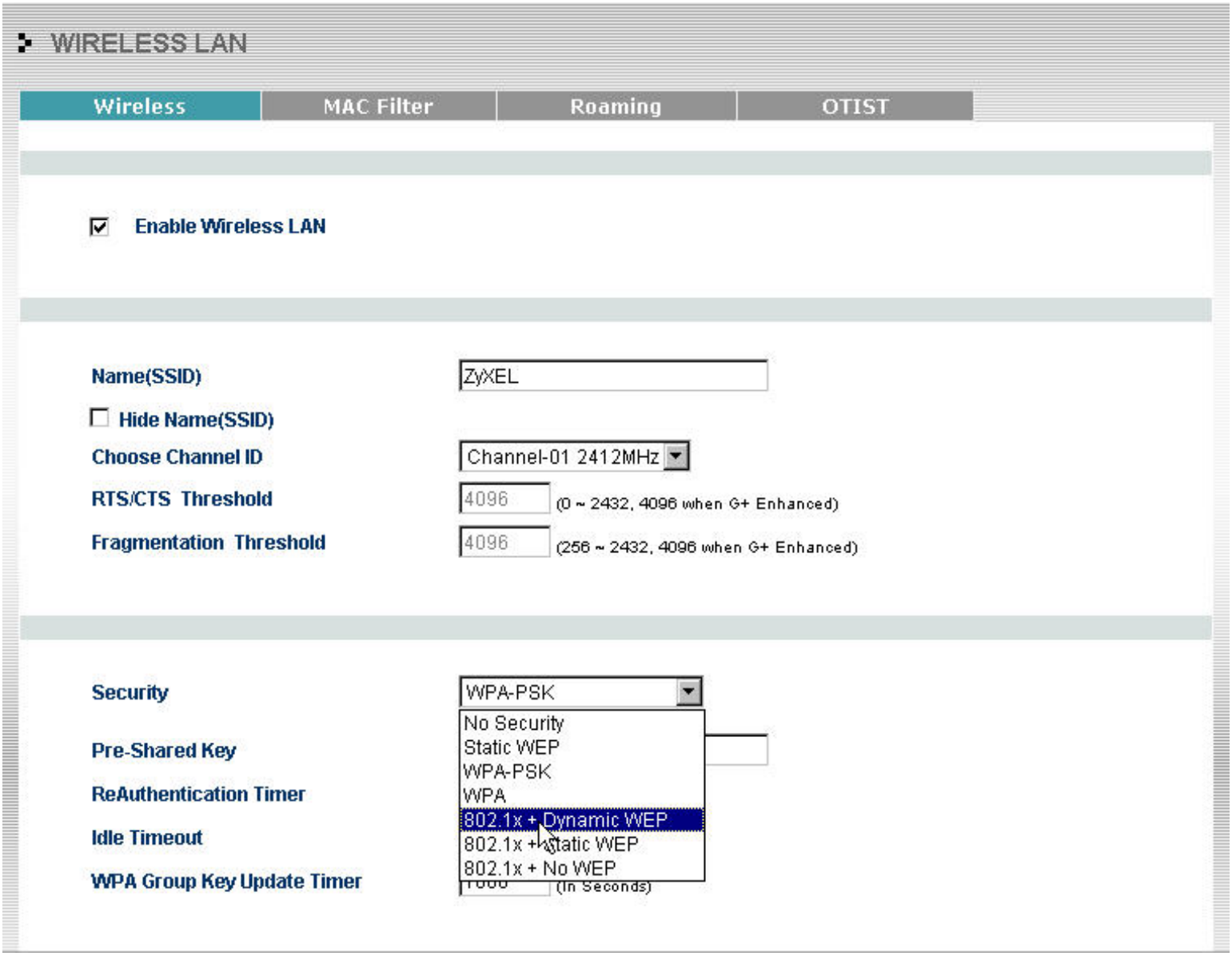
Authentication Control= **Auto/ Force Authorized/ Force UnAuthorized**
ReAuthentication Timer (in second)= 1800

Key Settings :

Option	Descriptions
Authentication Control	Press [SPACE BAR] to select from **Force Authorized, Force UnAuthorized** or **Auto**. The default is Force Authorized. **Auto :** Enables 802.1x function to authorize all wireless client, only the wireless client supported 802.1x client can access the network. **Force Authorized :** Disable 802.1x function, allow any wireless client access to your wireless network without authentication. **Force UnAuthorized :** Deny all wireless client access to your wireless network.
ReAuthentication Timer	Specify the time internal between authentication server's checks of wireless users connected to the network. The default time interval is **1800** seconds. This field is configurable when Authentication Control = Auto.

If you use WEB Configuration,

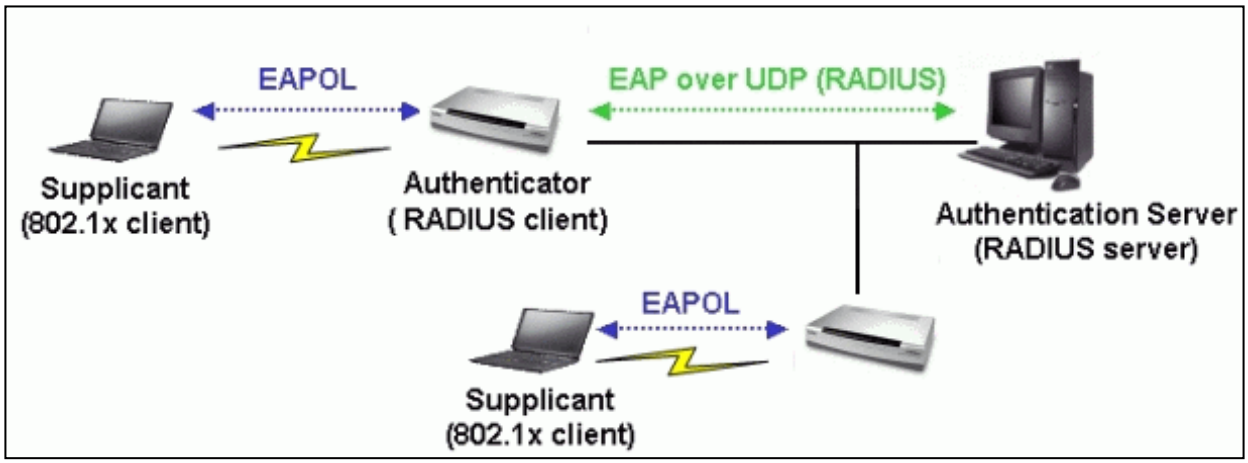
1. From the Web Configurator main menu, go to Main Menu/Wireless.
2. Select 802.1x authentication function.
3. Click **Apply** to make your setting work.



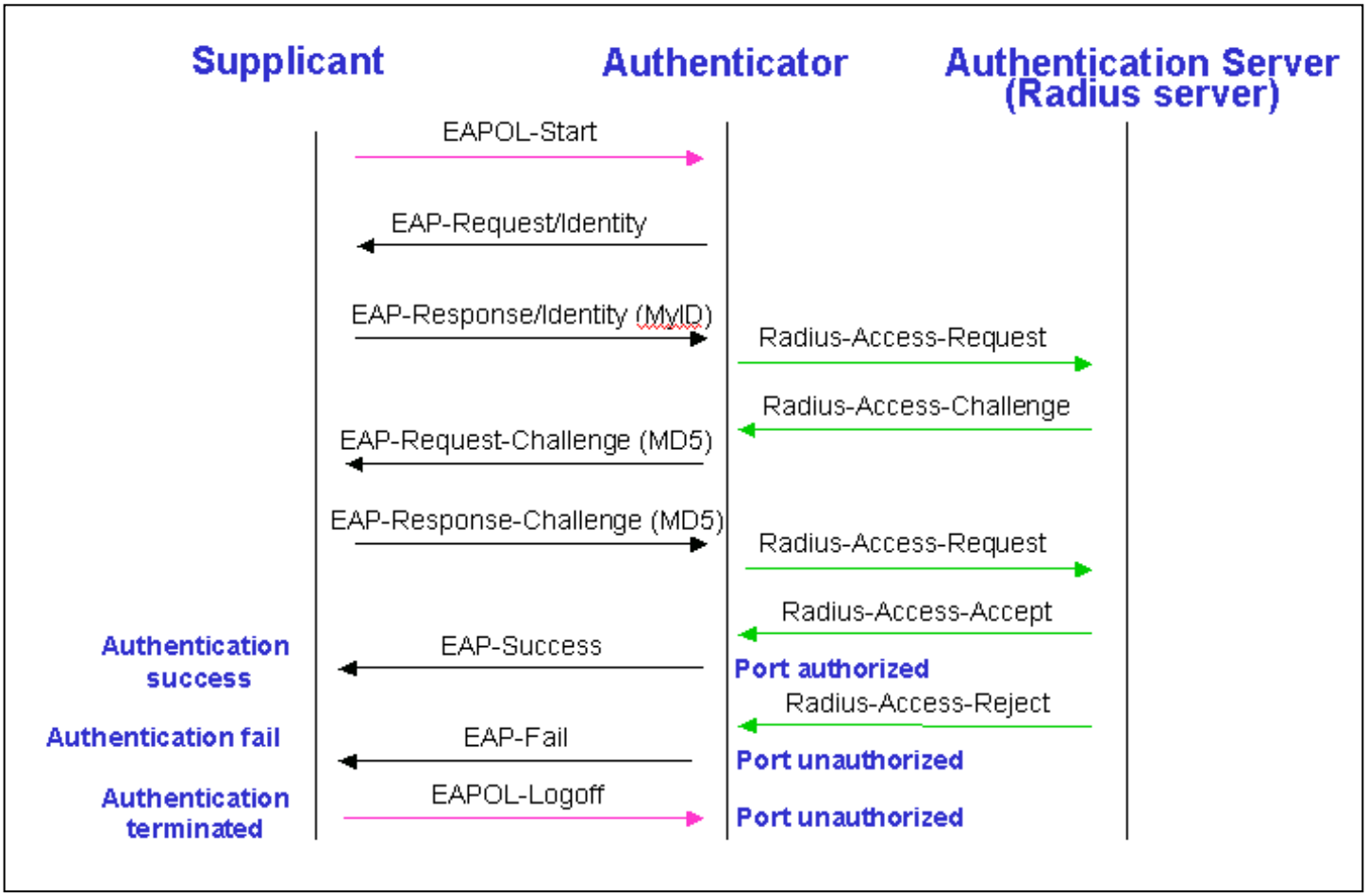
- ***Using External RADIUS Authentication Server***

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.

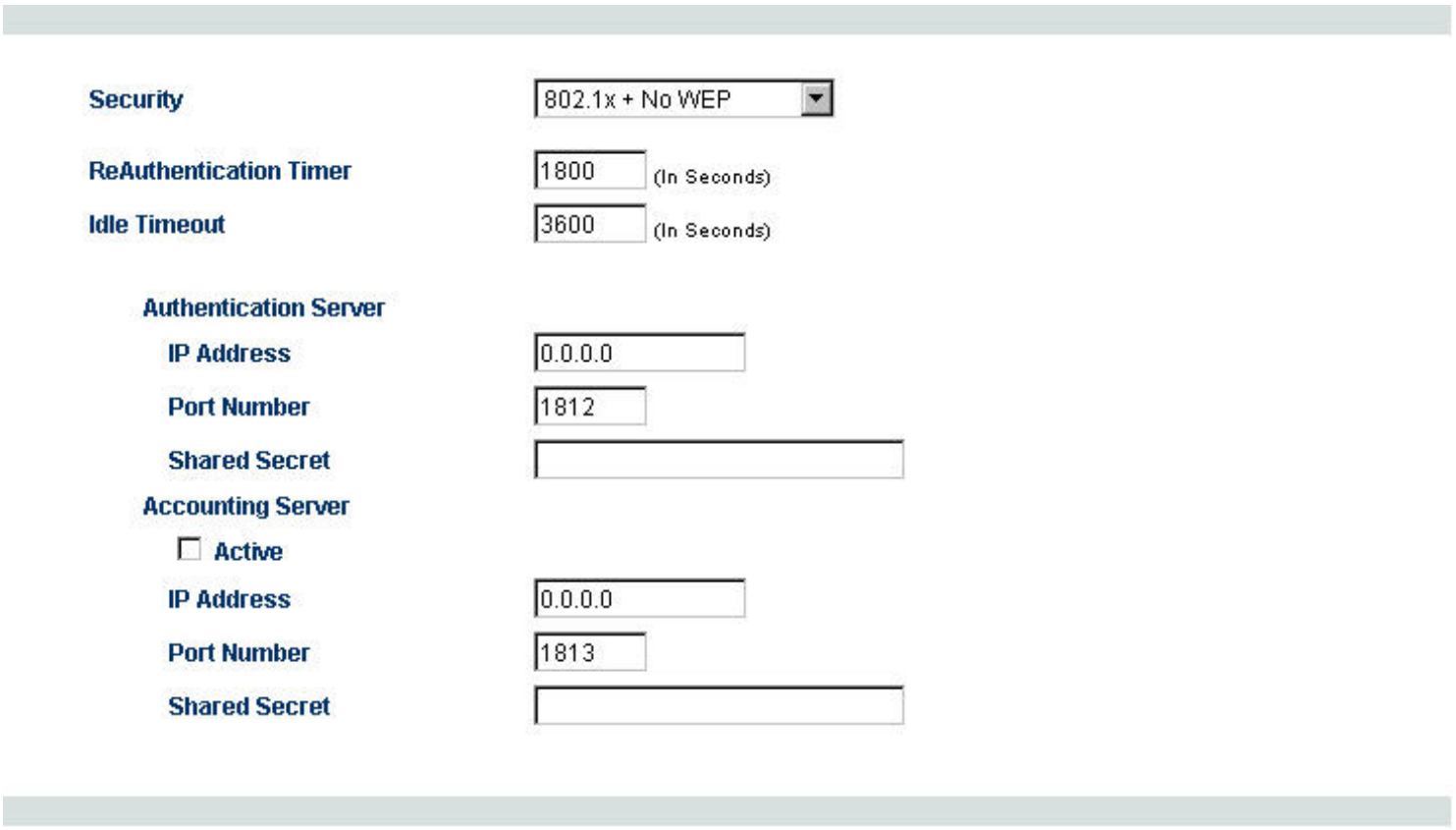
```
Menu 23.2 - System Security - RADIUS Server

        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
User Name	Enter a username up to 31 alphanumeric characters long.
Active	Press [SPACE BAR] to select **Yes** and press [Enter] to enable 802.1x user authentication through an external RADIUS authentication server. Select **No** to enable authentication using ZyXEL AP internal authentication server.
Server Address	Enter the IP address of the external RADIUS authentication server.
Port	The default port of RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	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, go to Main Menu/Wireless LAN/RADIUS to setup the RADIUS authentication and accounting server configuration.



Setup 802.1x client in the station

- Setup Windows XP 802.1x client
- Setup MeetingHouse AEGIS 802.1x client

- ***Setup 802.1x client in the station***

The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. So far, ZyXEL Wireless AP only supports MD-5 challenge authentication mechanism, but will support TLS and TTLS in the future. Here we just take MD-5 challenge authentication mechanism as a example.

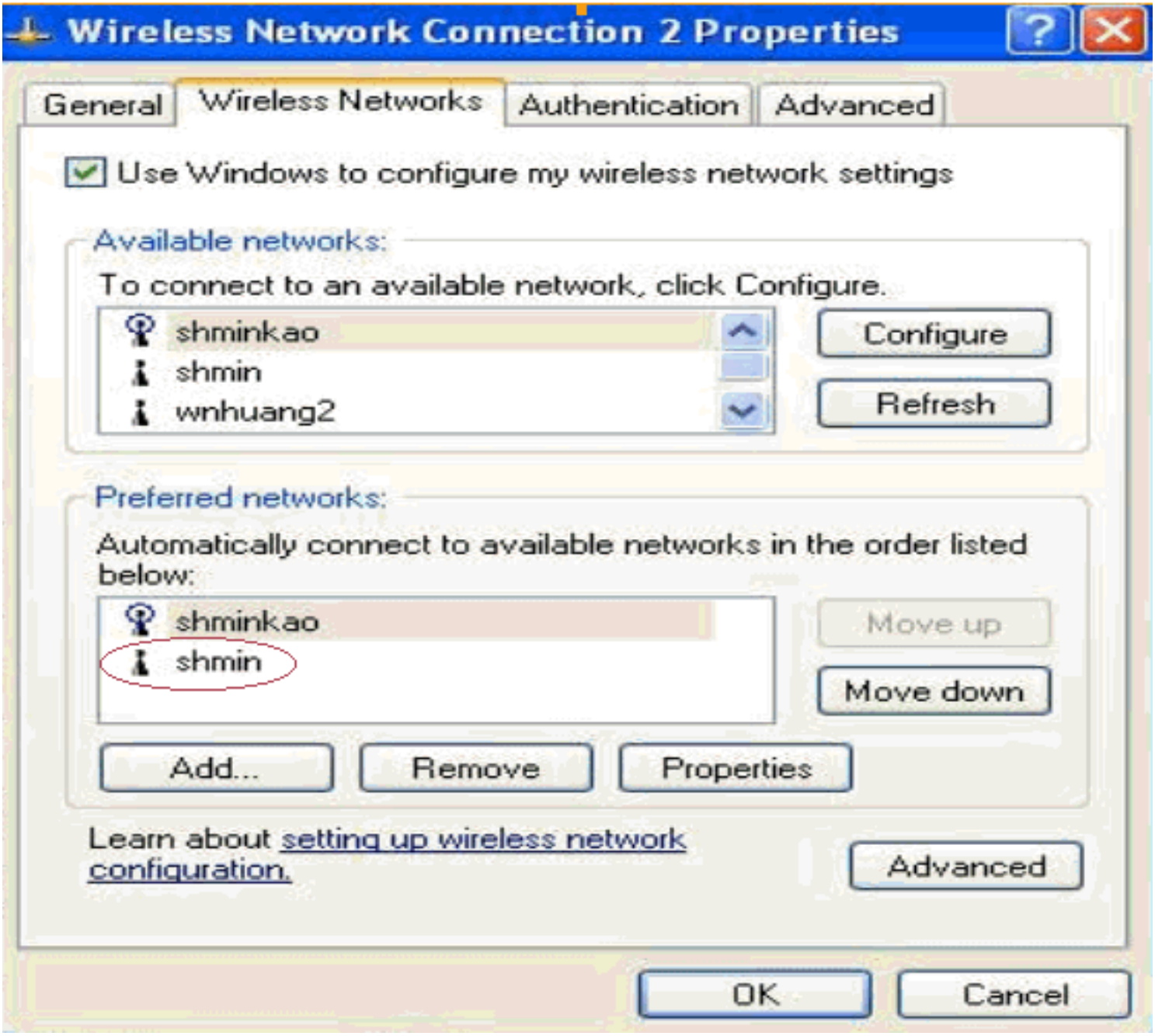
- ***Setup Windows XP 802.1x client***

Please install Windows XP that support 802.1x MD-5 challenge authentication mechanism. Don't upgrade to Service Pack 1, it support TLS authentication mechanism by default, instead of MD-5 challenge. ZyXEL Wireless AP will support TLS and TTLS in the future.

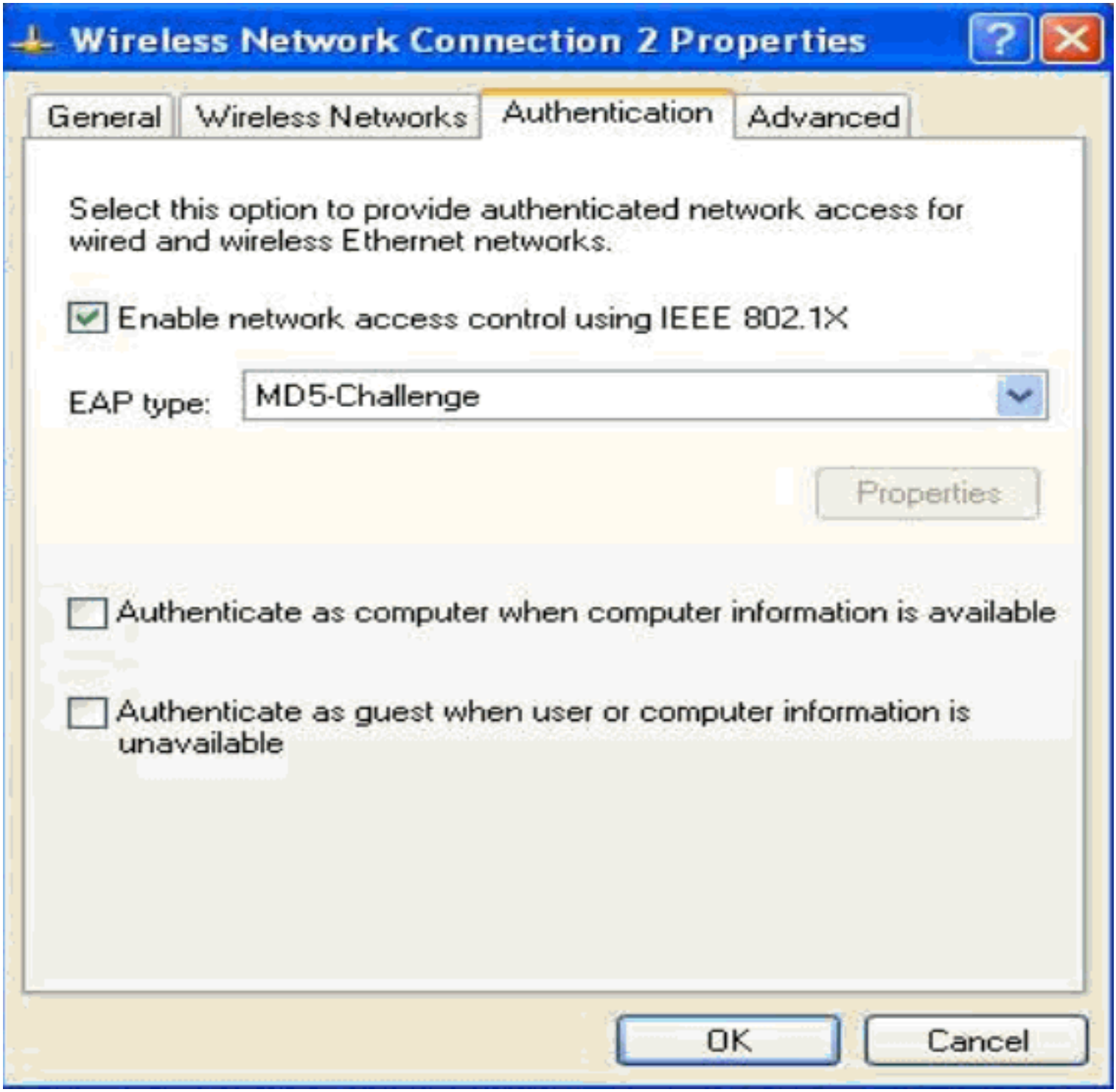
1.In the **Network** windows, choose **Wireless Network Connection** entry and click the **Properties** button.

2. In **Wireless Networks** tab, check **use windows to configure my wireless network**.

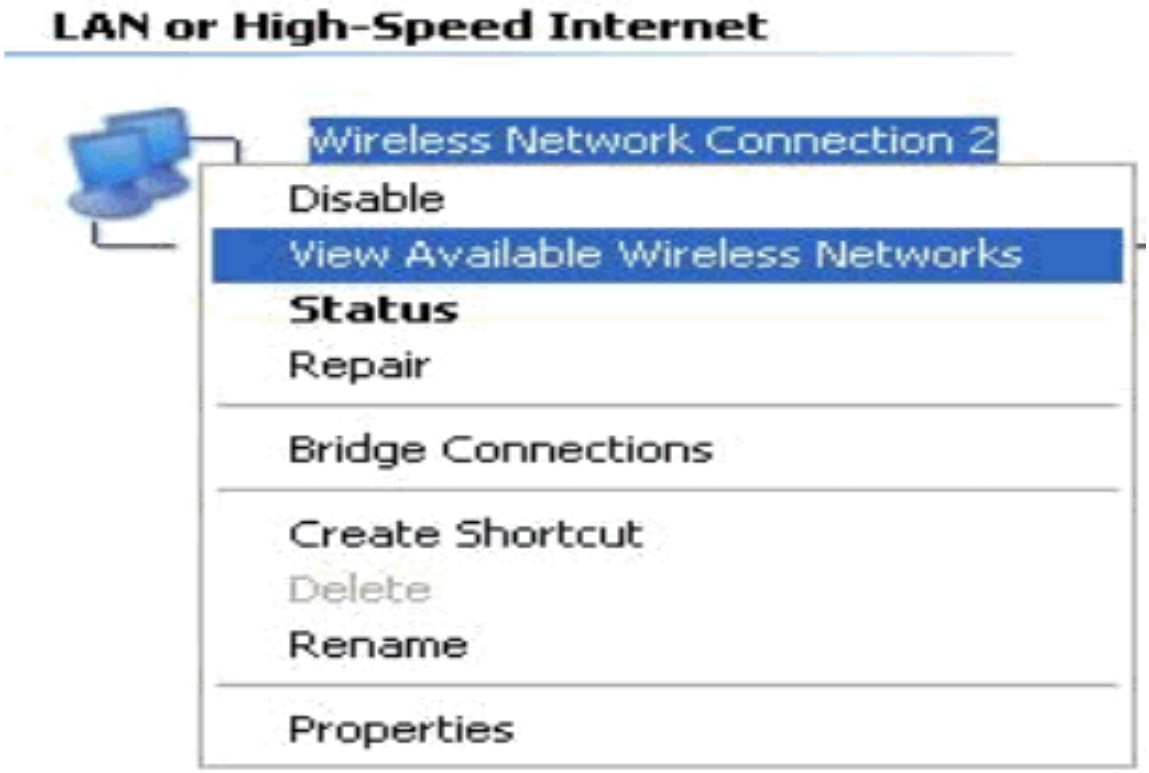
3. In **Preferred Networks** field, from the AP list found, move up the AP shmin (e.g.) that you want to use to the top by clicking on the **Move up** button (Windows XP will automatically detect the AP's ESSID and show it in **Available networks** field). If the AP is not shown in **Available networks** field, you can use the **Add...** button in **Preferred networks** to add the target AP into the list.



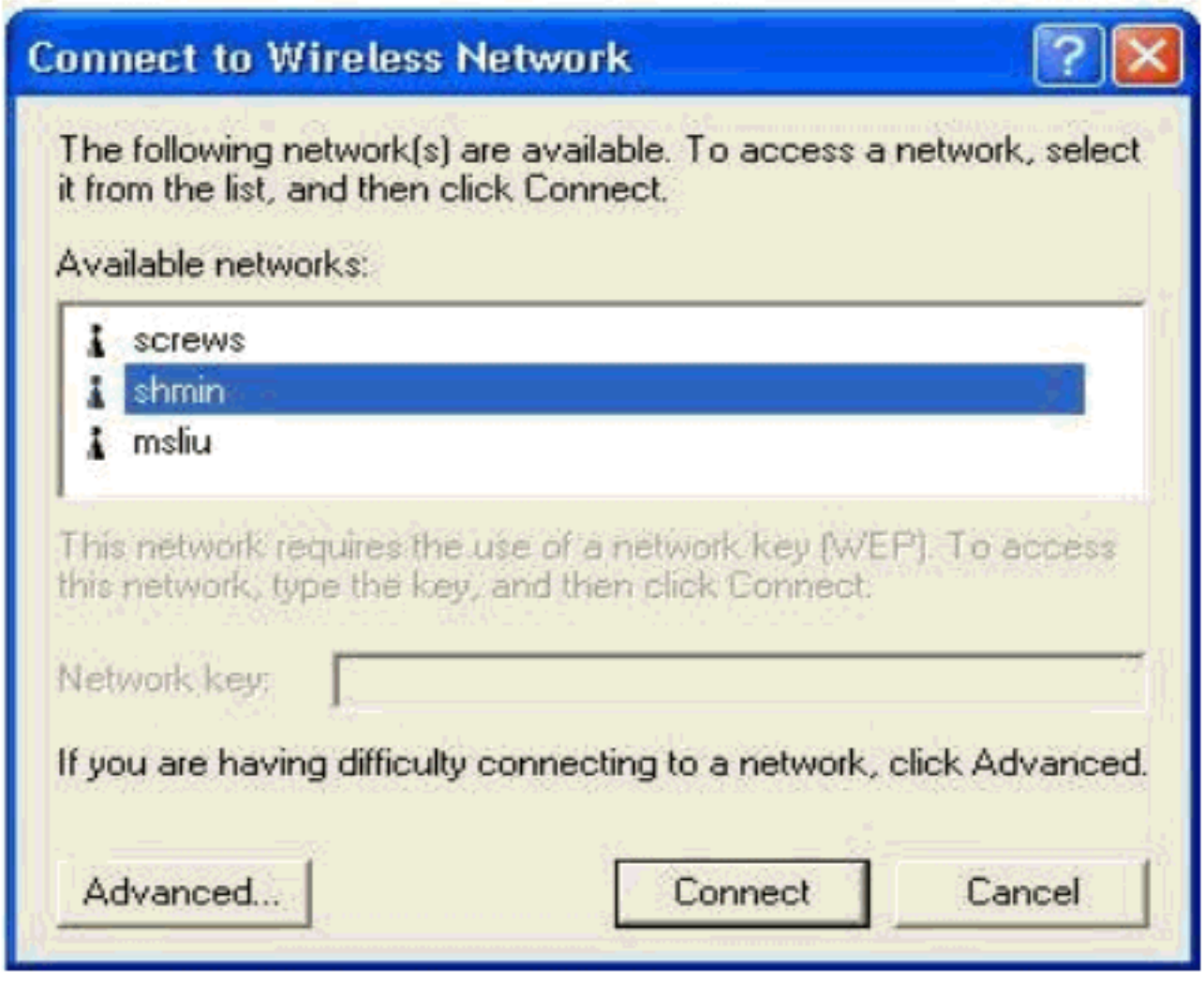
4. In **Authentication** tab, check **Enable network access control using IEEE 8021.x** and choose the **MD5-Challenge** in the **EAP type:** list, as shown below.



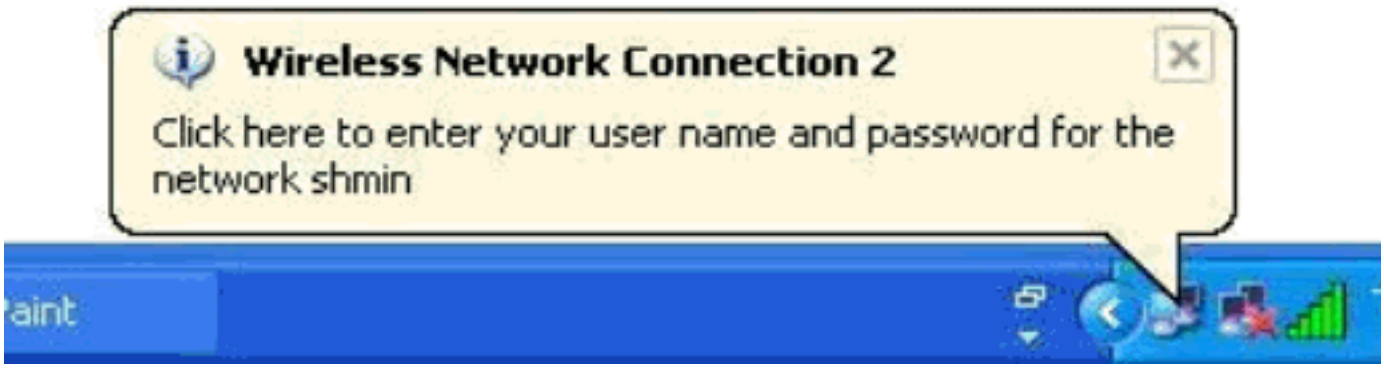
5. Connect to ZyXEL AP, in **Wireless Network Connection**, choose **View Available Wireless Networks**



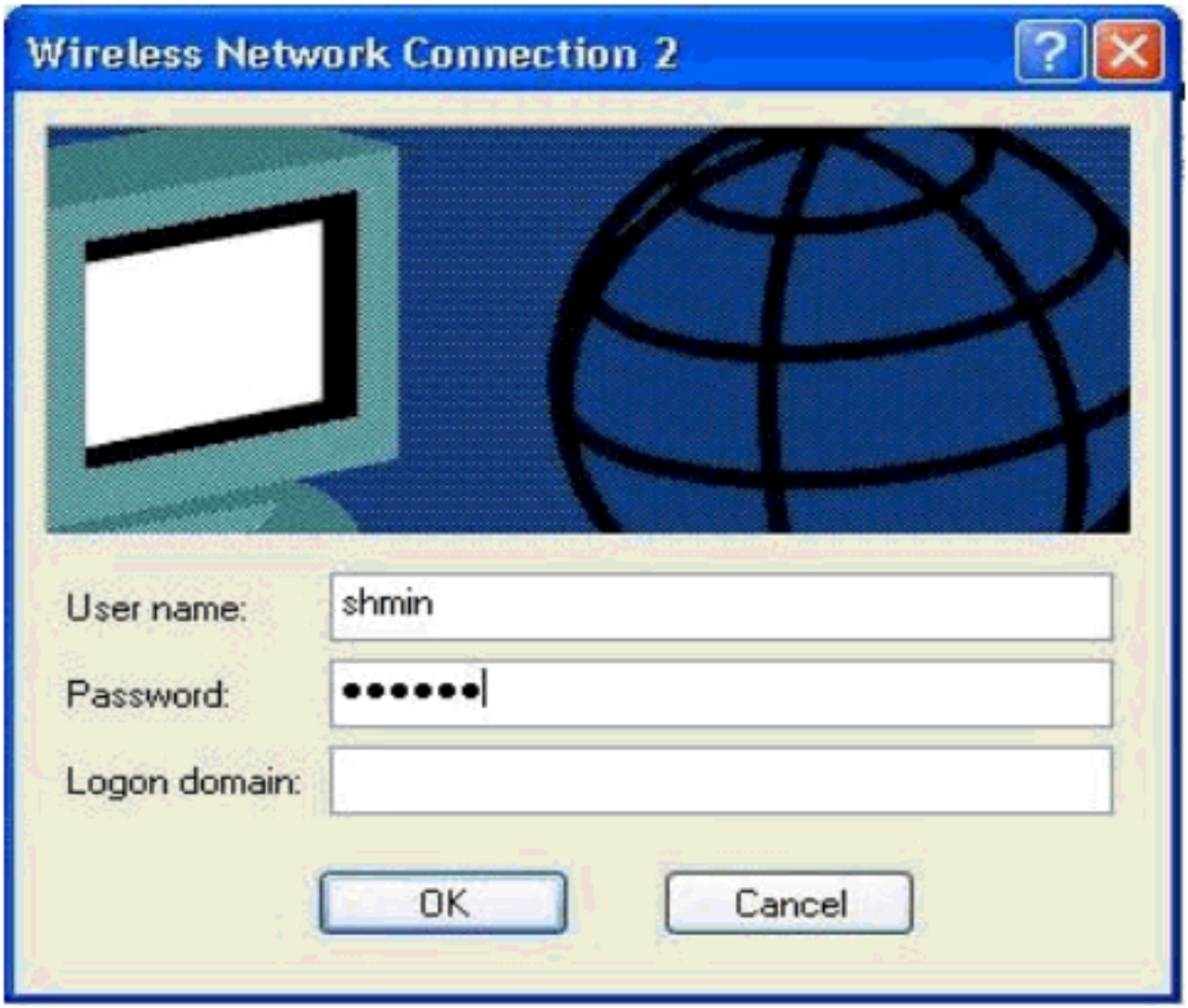
6. In the **Connect to Wireless Network** window, select the AP you would like to connect in the **Available networks** field then click **Connect** button for connection.



7. Windows XP will show you the message "**Click here to enter your user name and password for the network <AP_name>**" where the <AP_name> is the AP's name you chose on previous step. Click on the message box or the icon shown on the icon list.



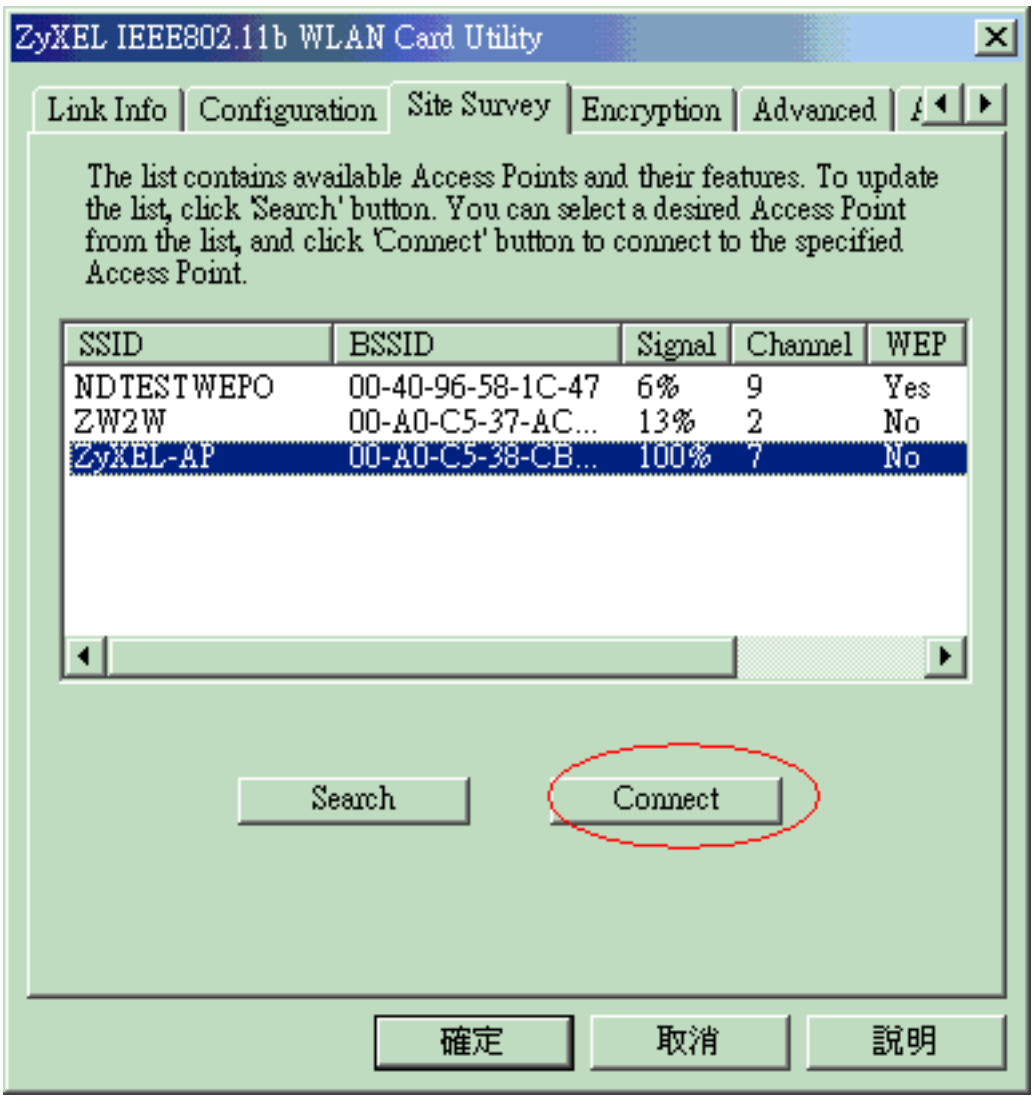
8. In the **Wireless Network Connection** window, enter the <user_name> in the **User name** field and <pass_word> in the **Password** field that are already set in AP for login. Click **OK** to finish the connection.



9. Windows XP completes the negotiation and changes the status for you automatically as shown on following figure.

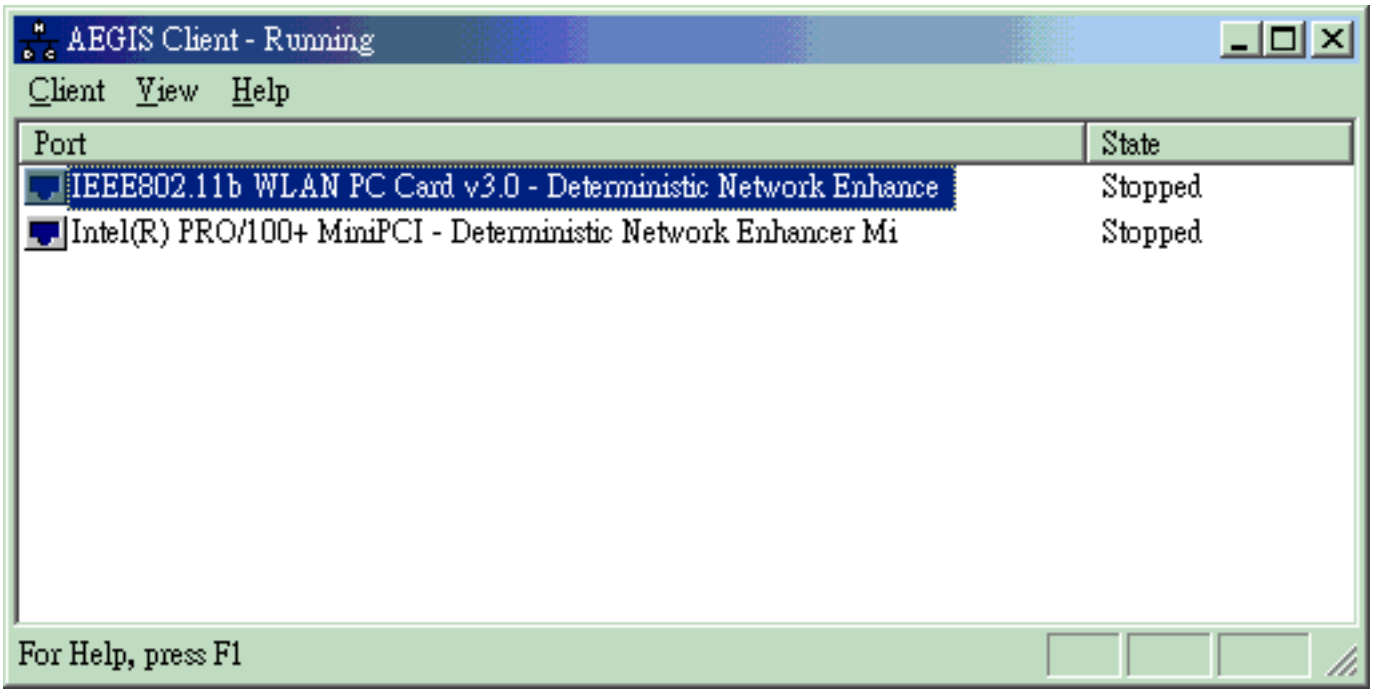
- ***Setup MeetingHouse AEGIS 802.1x client***

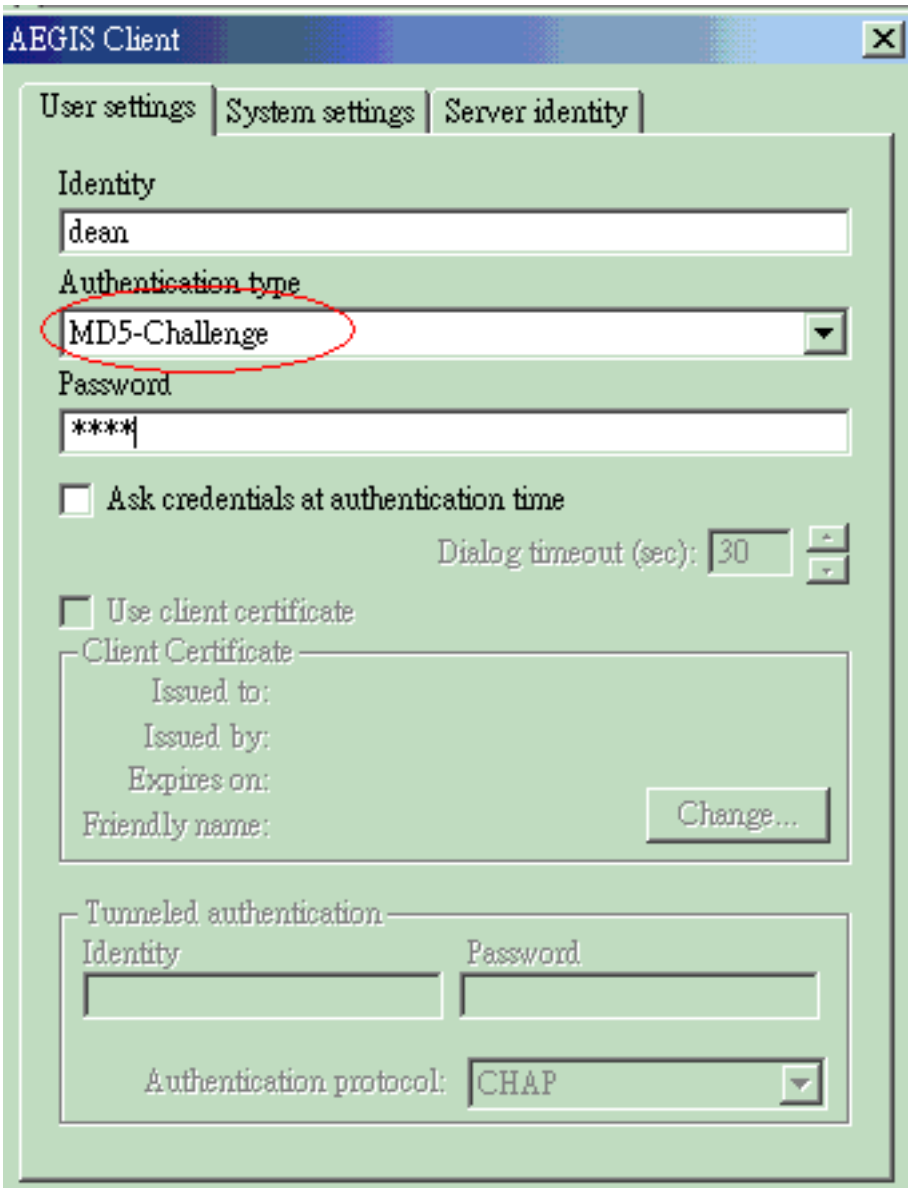
1. Please connect your wireless client to AP before configuring AEGIS 802.1x client.



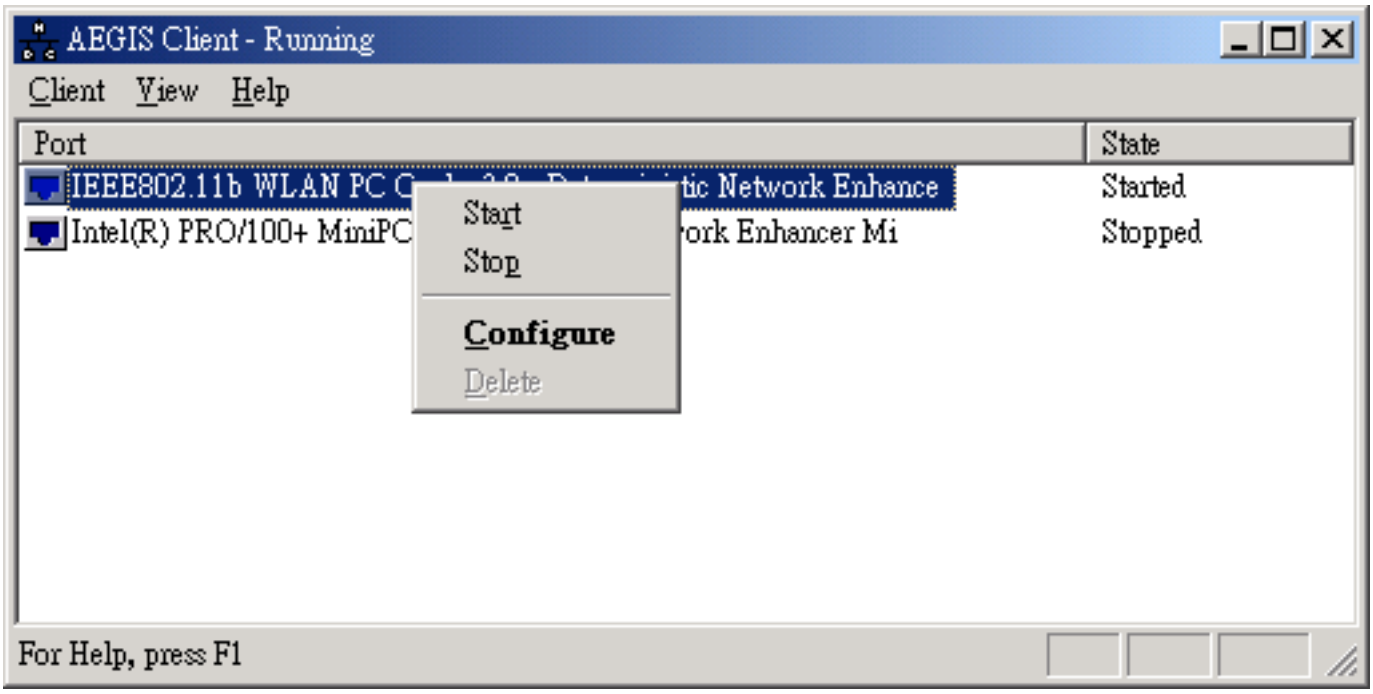
2. Open **AEGIS Client- Running** window, choose **Client** --> **Configure** --> Select **User settings** tag --> Type the username into the **Identity** field --> Select **MD5-Challenge authentication type** --> Type password into **Password** field --> Click **Apply** button to save your configuration and return

to AEGIS Client window.





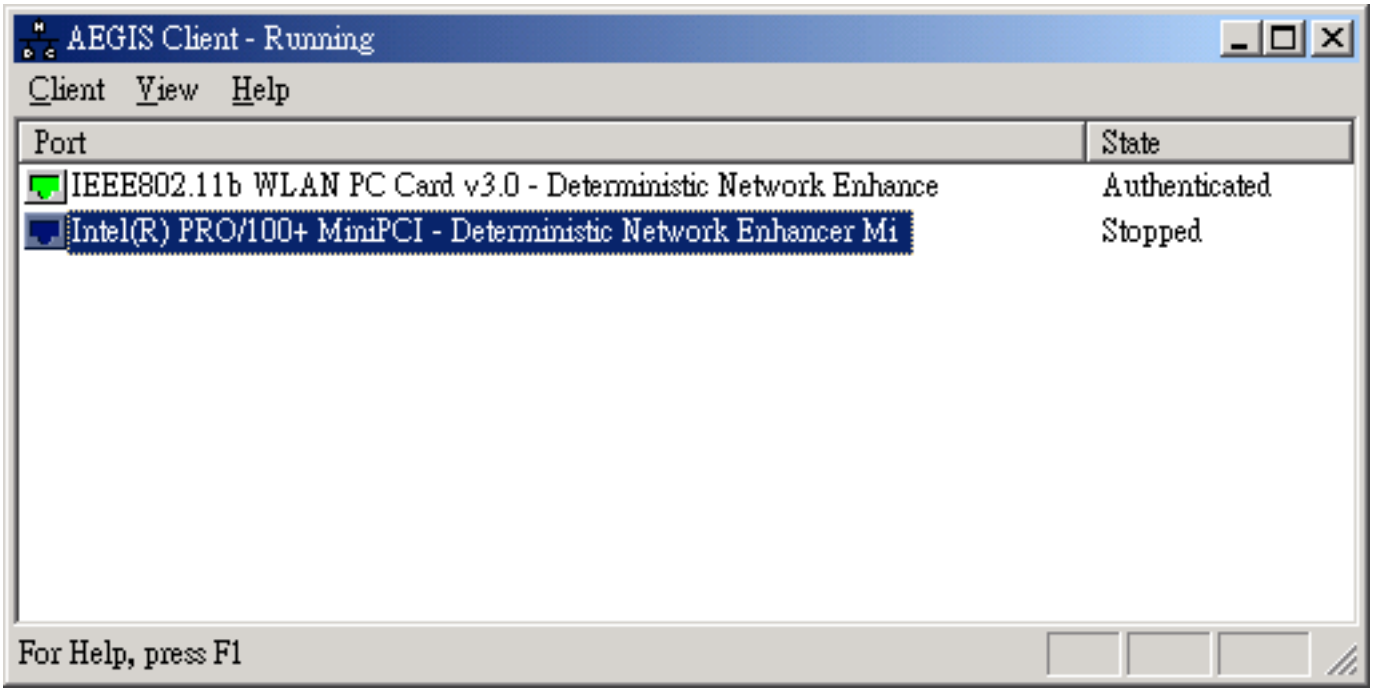
3. Right click the specified wireless client adapter in the AEGIS Client --> Select **Start** to start the 802.1x authentication on the specified wireless clinet adapter.



4. AEGIS 8021.x client completes the negotiation and changes status automatically.

Before 802.1x authentication :

After 802.1x authentication is completed :



5. If AEGIS 802.1x client does not start to negotiate with wireless AP, please perform Step 1 again.

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.

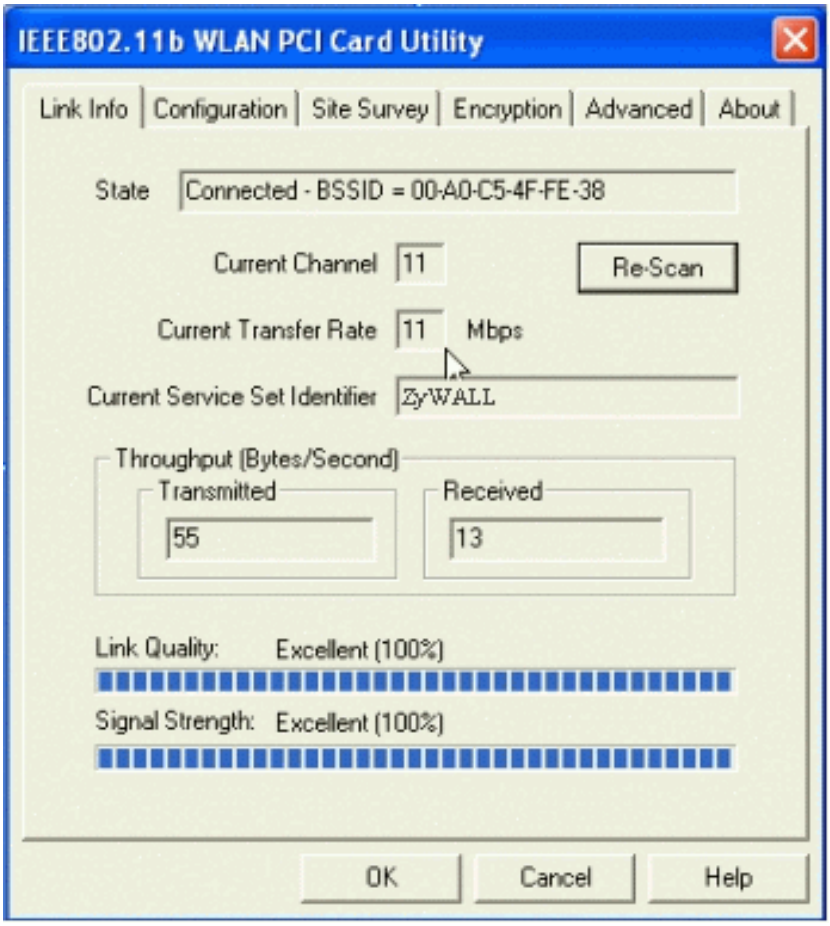
4. Determine the preliminary access point location on the facility diagram base on the service area needed, obstacles, power wall jack considerations.

Survey on Site

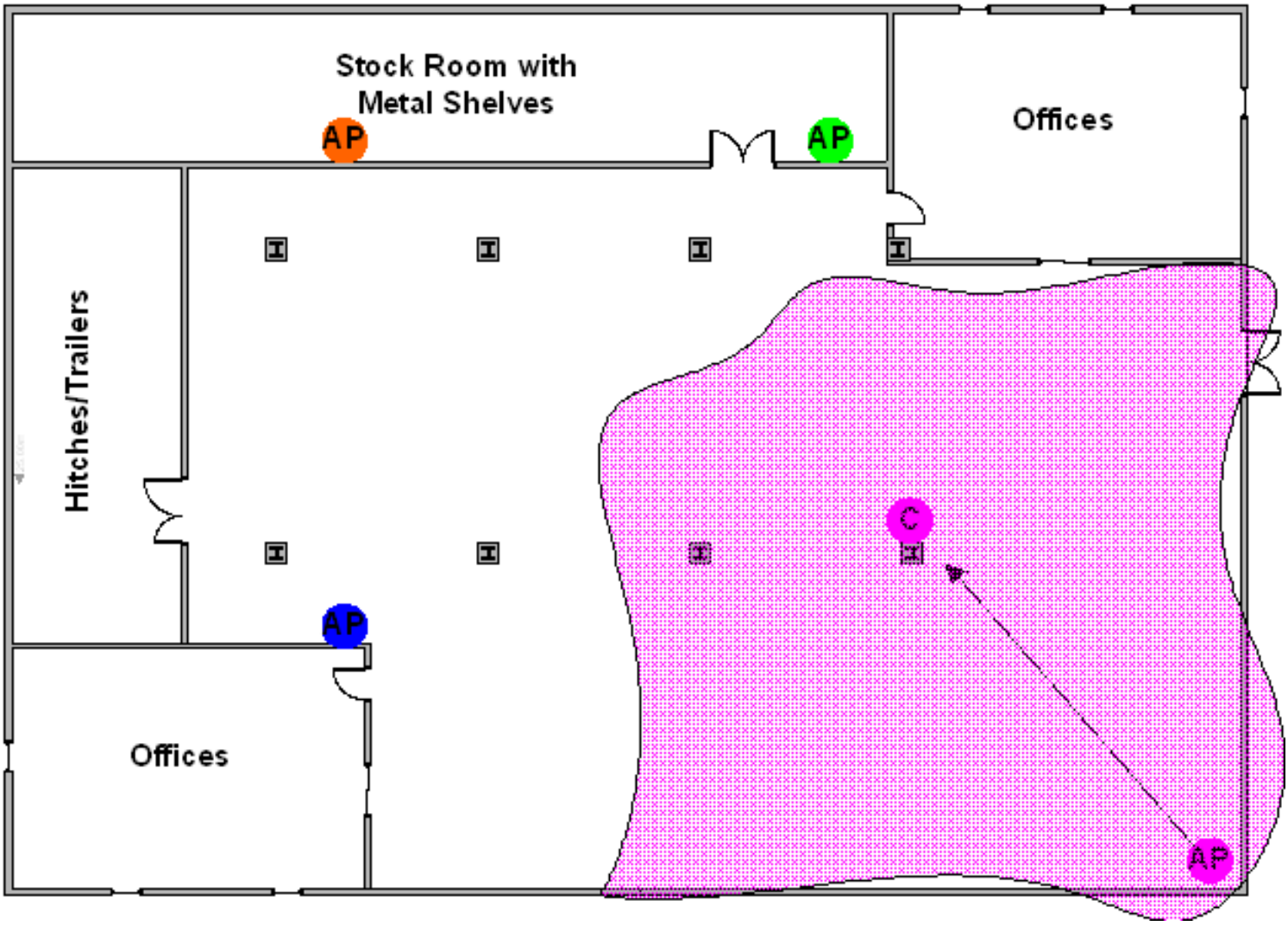
1. With the diagram with all information you gathered in the preparation phase. Now you are ready to make the survey.

2. Install an access point at the preliminary location.

3. User 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.

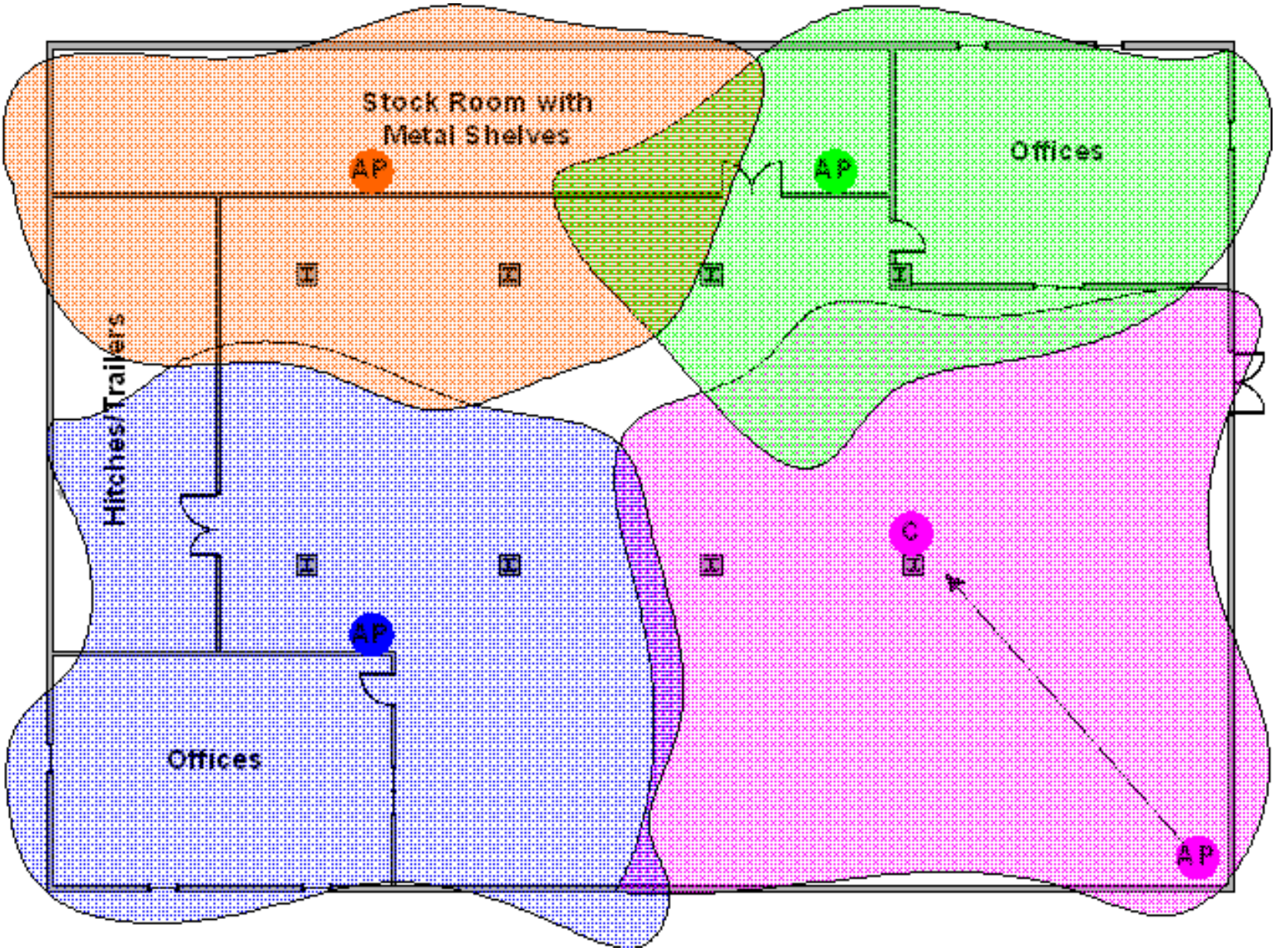


5. When you reach the farthest point of connection mark the spot. Now you move the access point to this new spot as have already determine the farthest point of the access point installation spot if wireless service is required from corner of the room.

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

TMSS Application Notes

- Registration Steps(Demo)
- FAQ

TMSS

- TMSS Introduction
- TMSS Registration Demo

- ***TMSS Introduction***

  What is TMSS?

Help to identify vulnerabilities and to protect PCs and networks that are connected to the Internet via a router.

Integrated with chosen hardware partners, TMSS is designed to address the security needs of PCs that access the Internet via broadband routers.

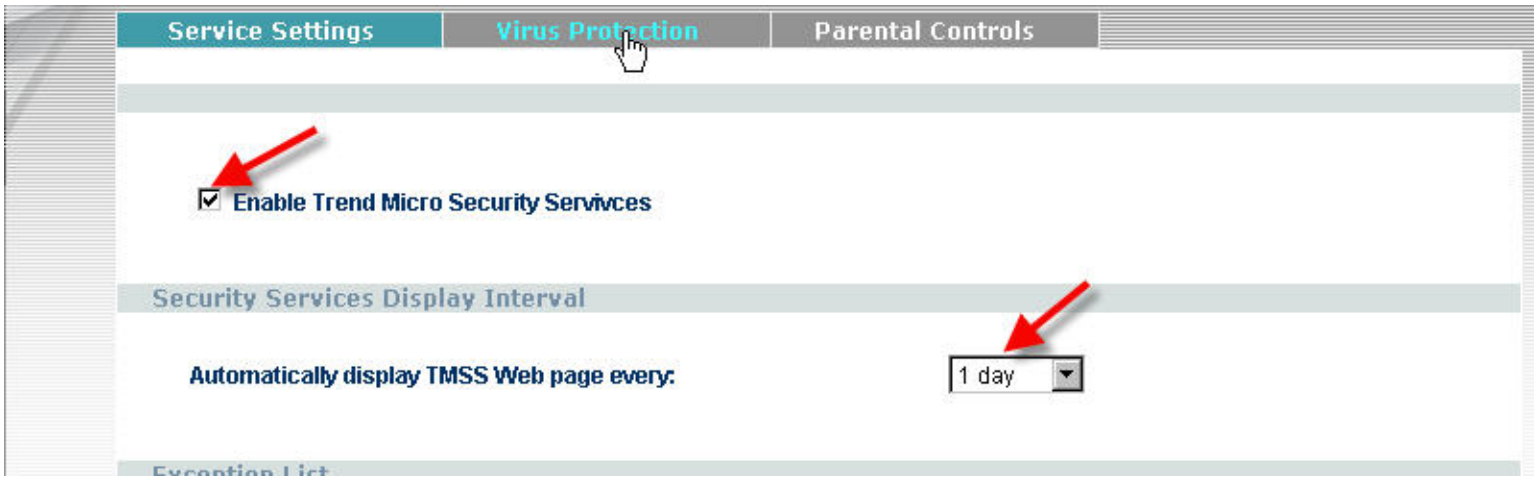
TMSS provides benefits which includes the following :

1. Security Report via Security Scan

2. Trend Micro Internet Security
3. Parental Controls

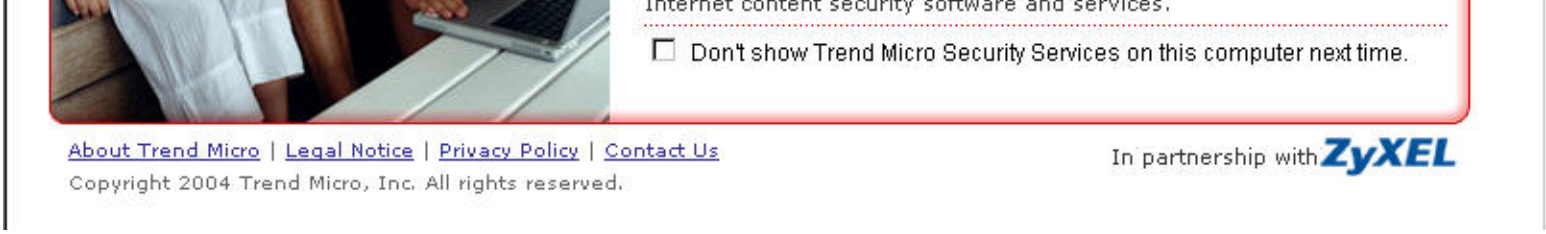
TMSS Registration Demo.

1. In Web GUI Advance/TMSS, enable the TMSS service. Also you can configure the interval time for displaying TMSS web page. (before this procedure, please make sure that the setting for Internet access is proper.)

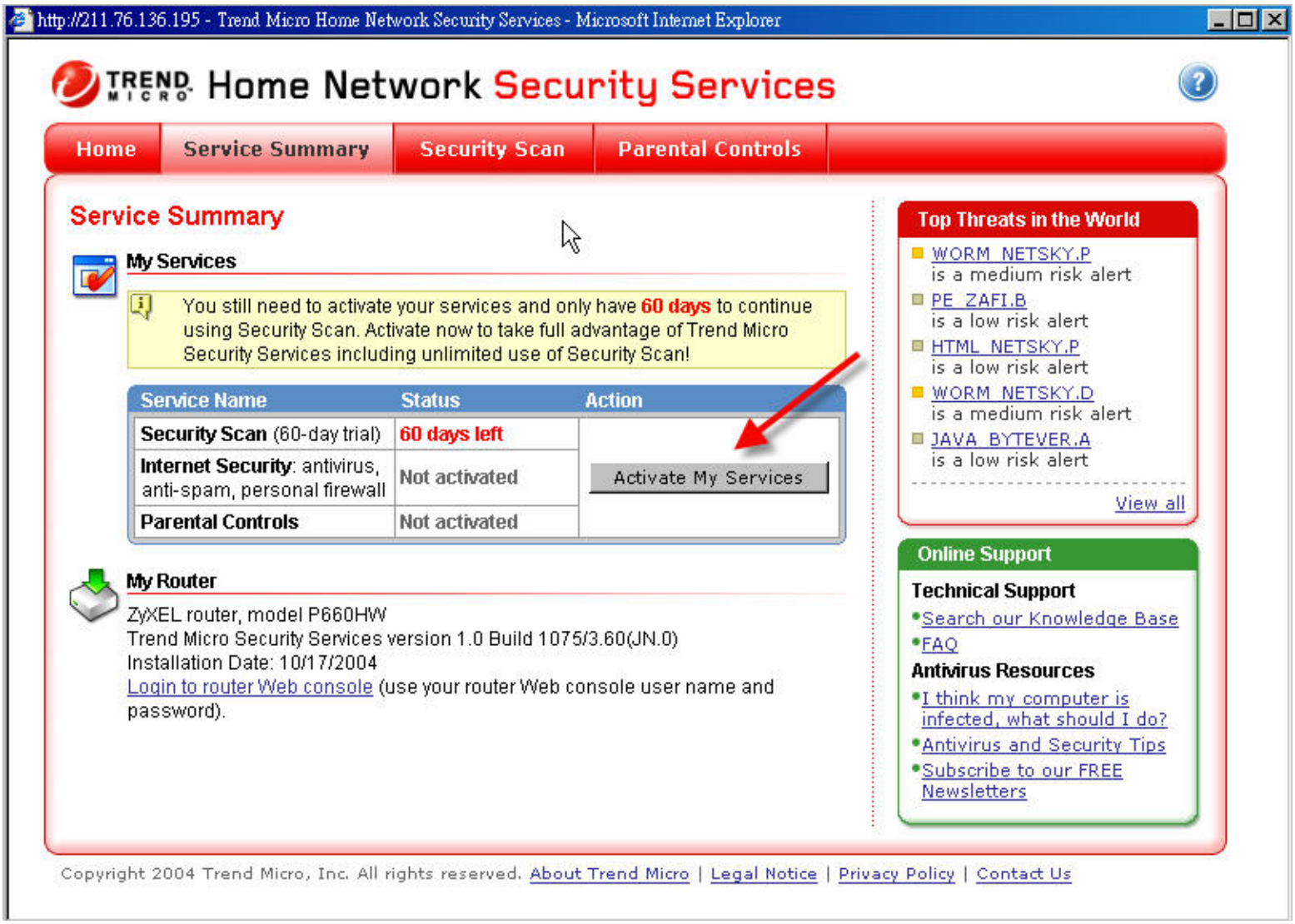


2. Client under LAN of the device open the Web Browser (IE), there will pop-up one window to instruct you to install Active-X from TMSS. After you install the Active-X, the window will change as below. (Please notice some program or Win XP SP2 will block pop-up window, so before registration, please turn off this kind of function.)

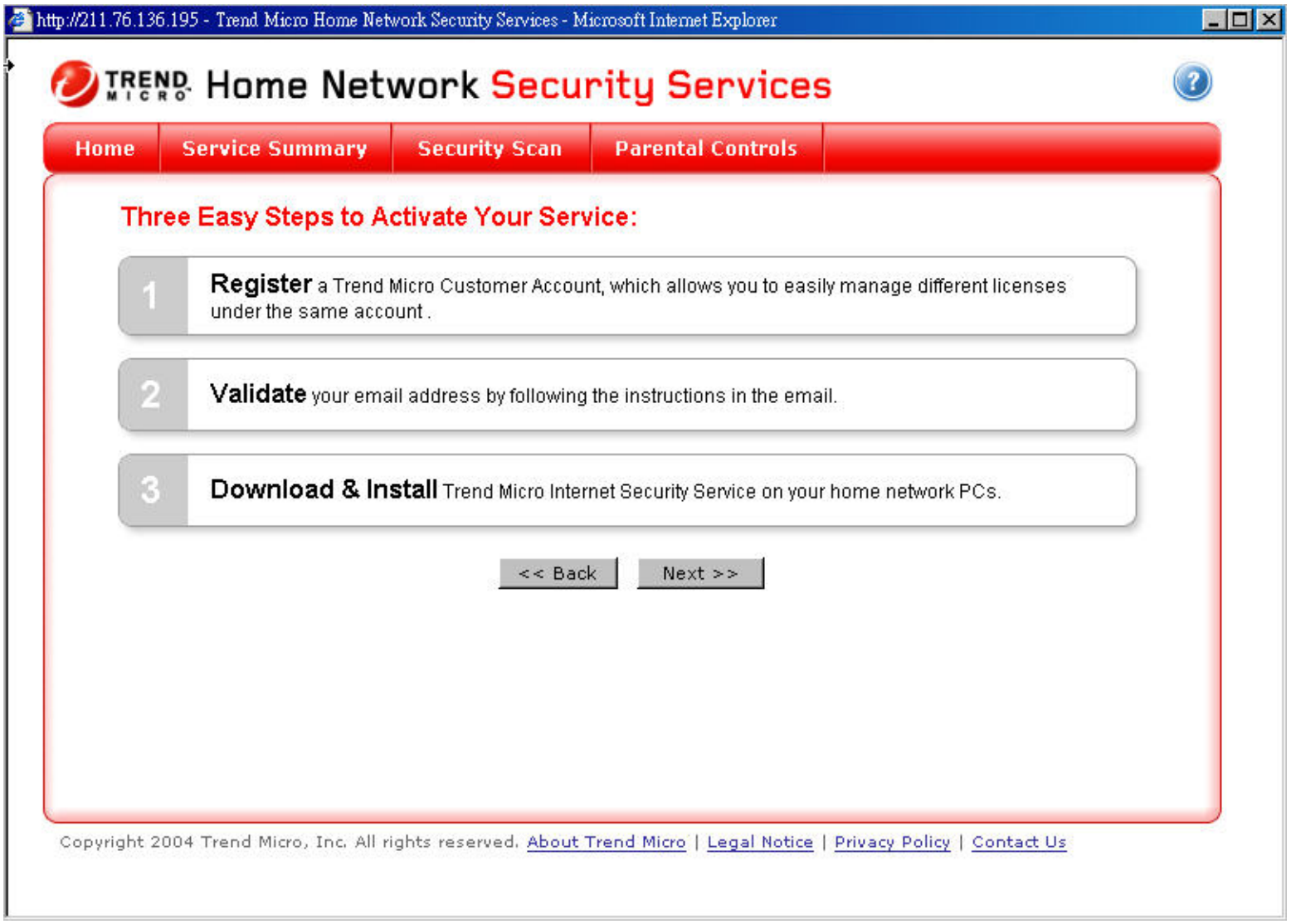
3. When you apply "Continue" button, the web page will redirect to TMSS dashboard as below.

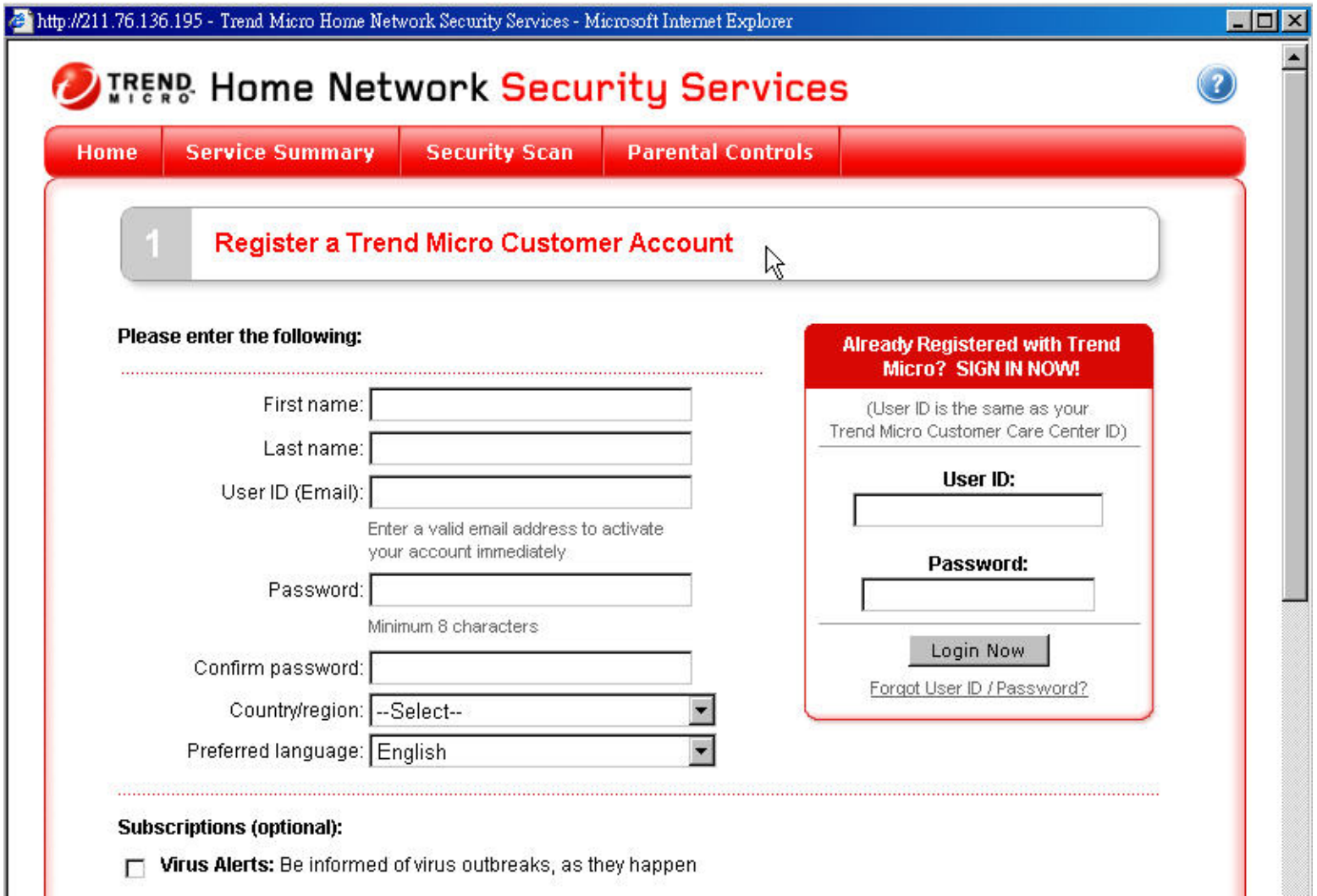


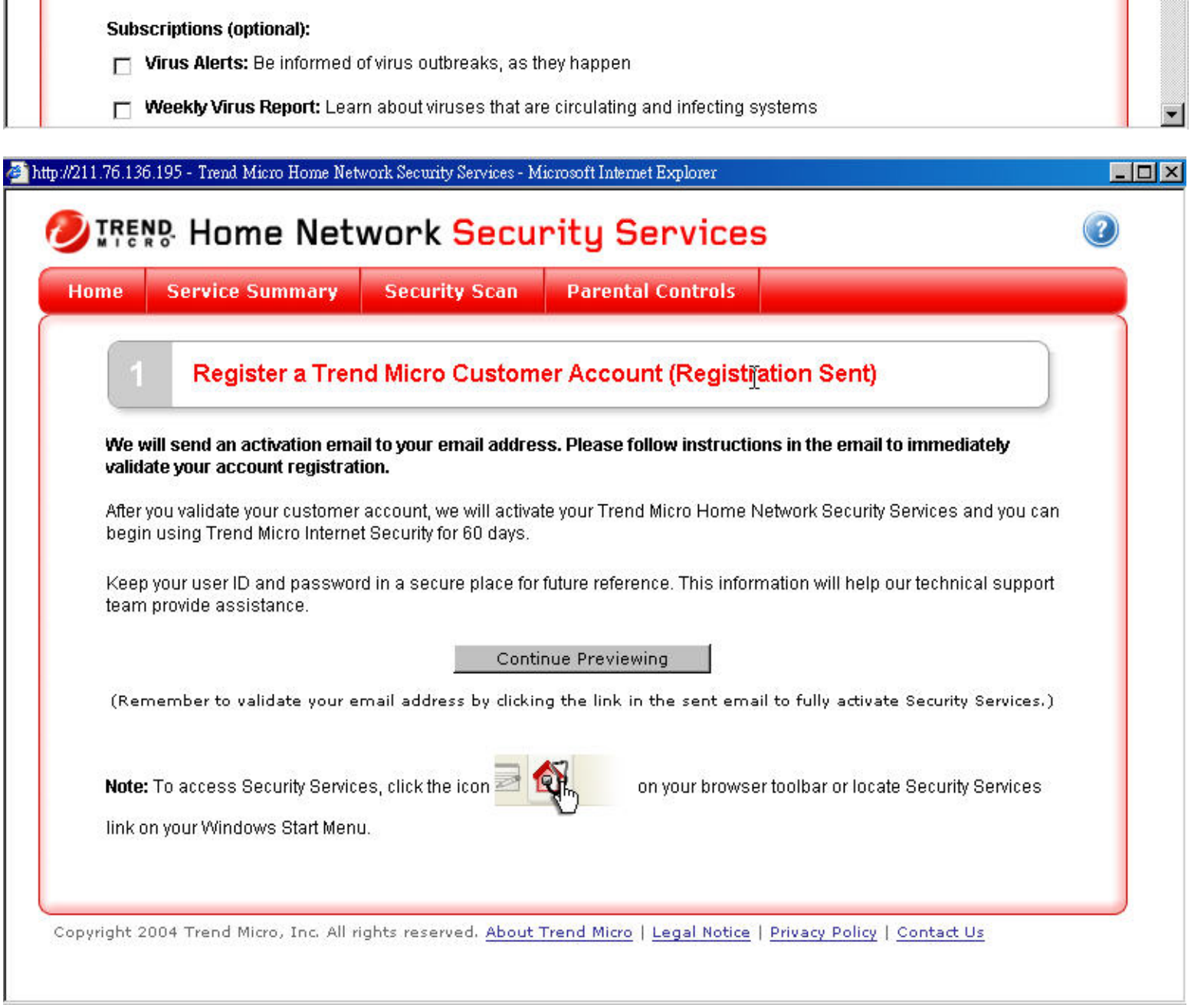
4. Click "Service Summary", in this page you can activate the TMSS service. (You can press the "?" mark in the page for more detail information)



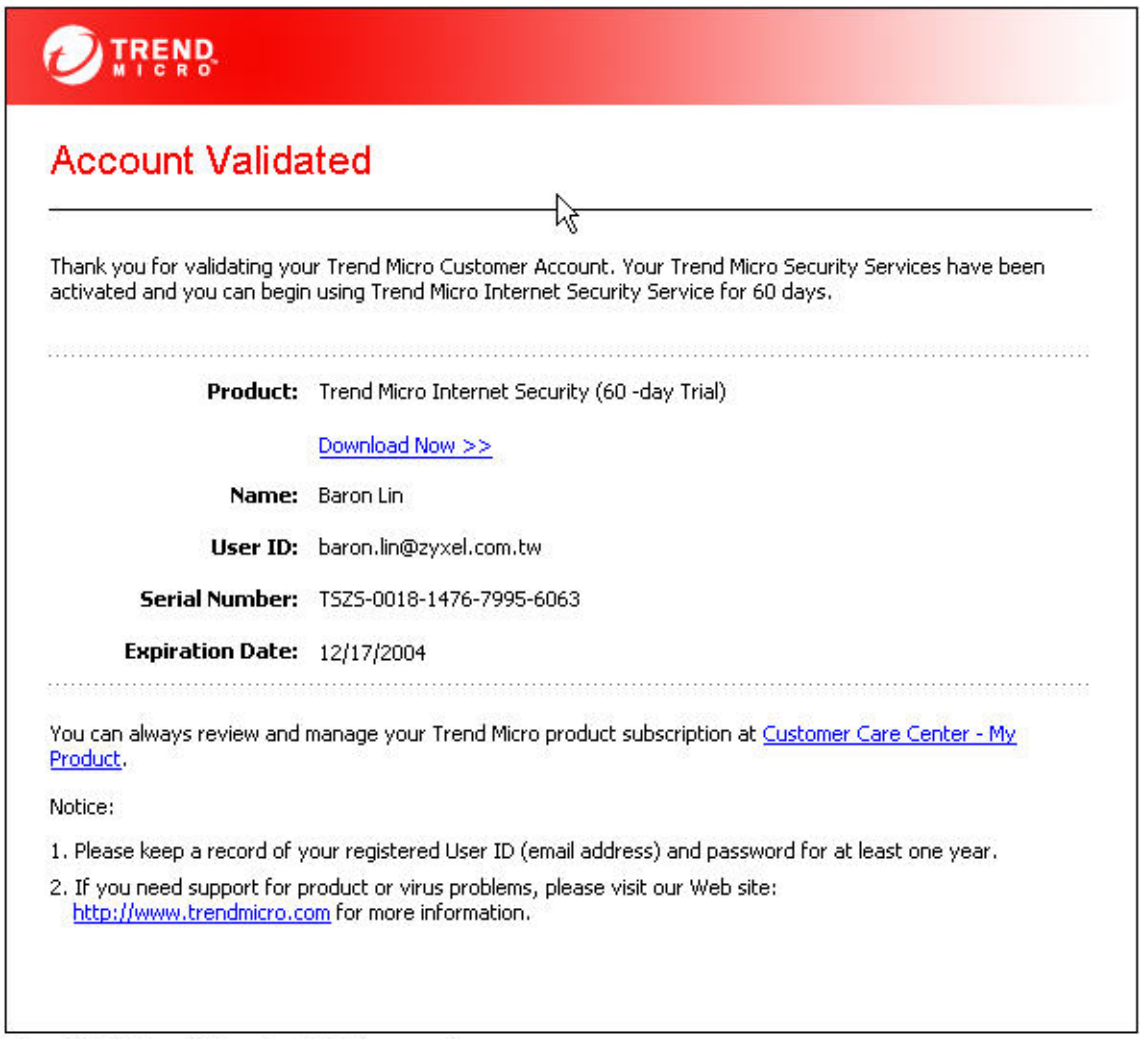
5. Click "Activate My Services", you will receive the pages below. (Please follow instruction in the page to finish the steps of registration.)


http://211.76.136.195 - Trend Micro Home Network Security Services - Microsoft Internet Explorer
TREND MICRO Home Network Security Services
Home
Service Summary
Security Scan
Parental Controls
Three Easy Steps to Activate Your Service:
1 Register a Trend Micro Customer Account, which allows you to easily manage different licenses under the same account .
2 Validate your email address by following the instructions in the email.
3 Download & Install Trend Micro Internet Security Service on your home network PCs.
<< Back
Next >>
Copyright 2004 Trend Micro, Inc. All rights reserved. About Trend Micro | Legal Notice | Privacy Policy | Contact Us

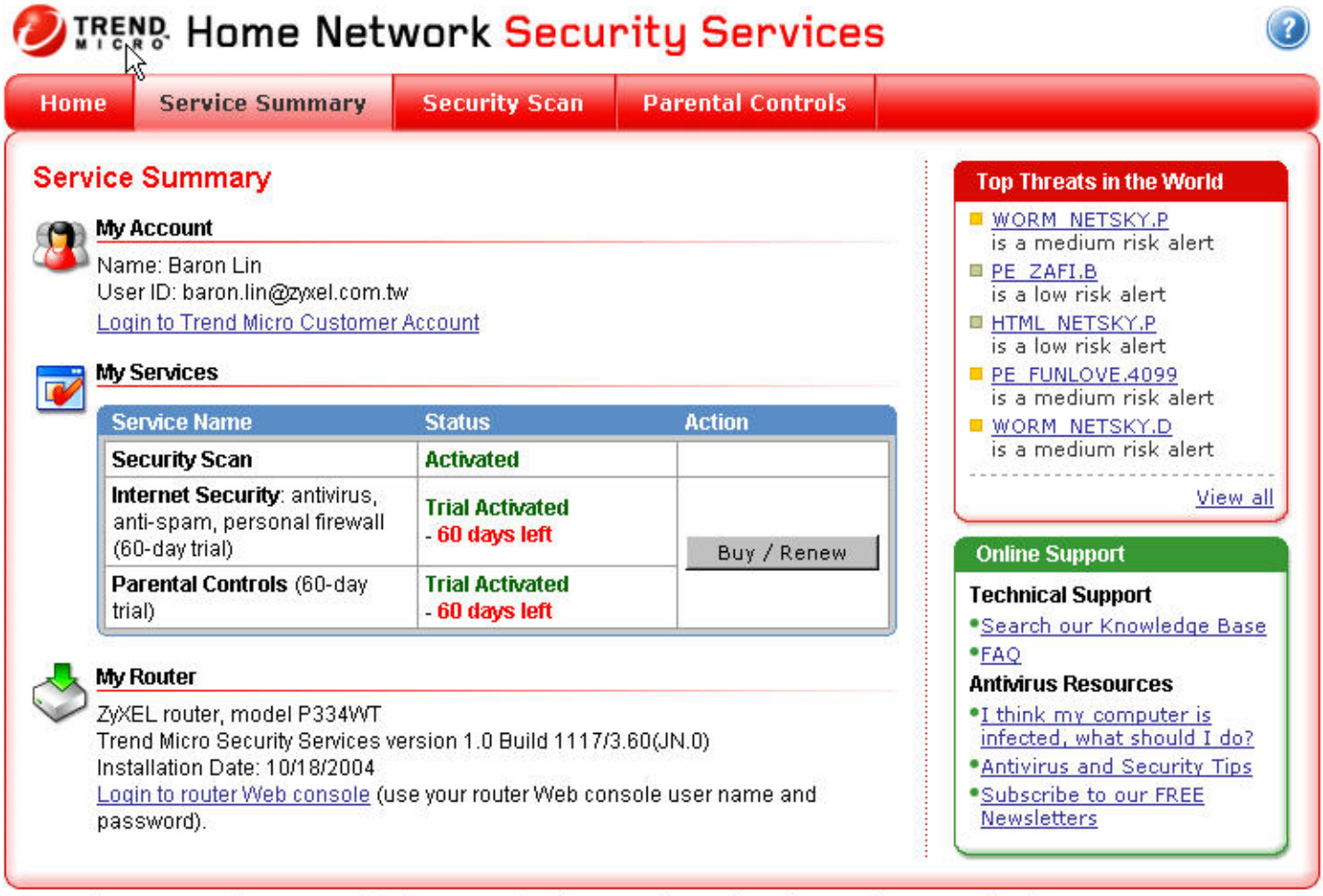

http://211.76.136.195 - Trend Micro Home Network Security Services - Microsoft Internet Explorer
TREND MICRO Home Network Security Services
Home
Service Summary
Security Scan
Parental Controls
1 Register a Trend Micro Customer Account
Please enter the following:
First name:
Last name:
User ID (Email):
Enter a valid email address to activate your account immediately
Password:
Minimum 8 characters
Confirm password:
Country/region: --Select--
Preferred language: English
Already Registered with Trend Micro? SIGN IN NOW!
(User ID is the same as your Trend Micro Customer Care Center ID)
User ID:
Password:
Login Now
Forgot User ID / Password?
Subscriptions (optional):
Virus Alerts: Be informed of virus outbreaks, as they happen

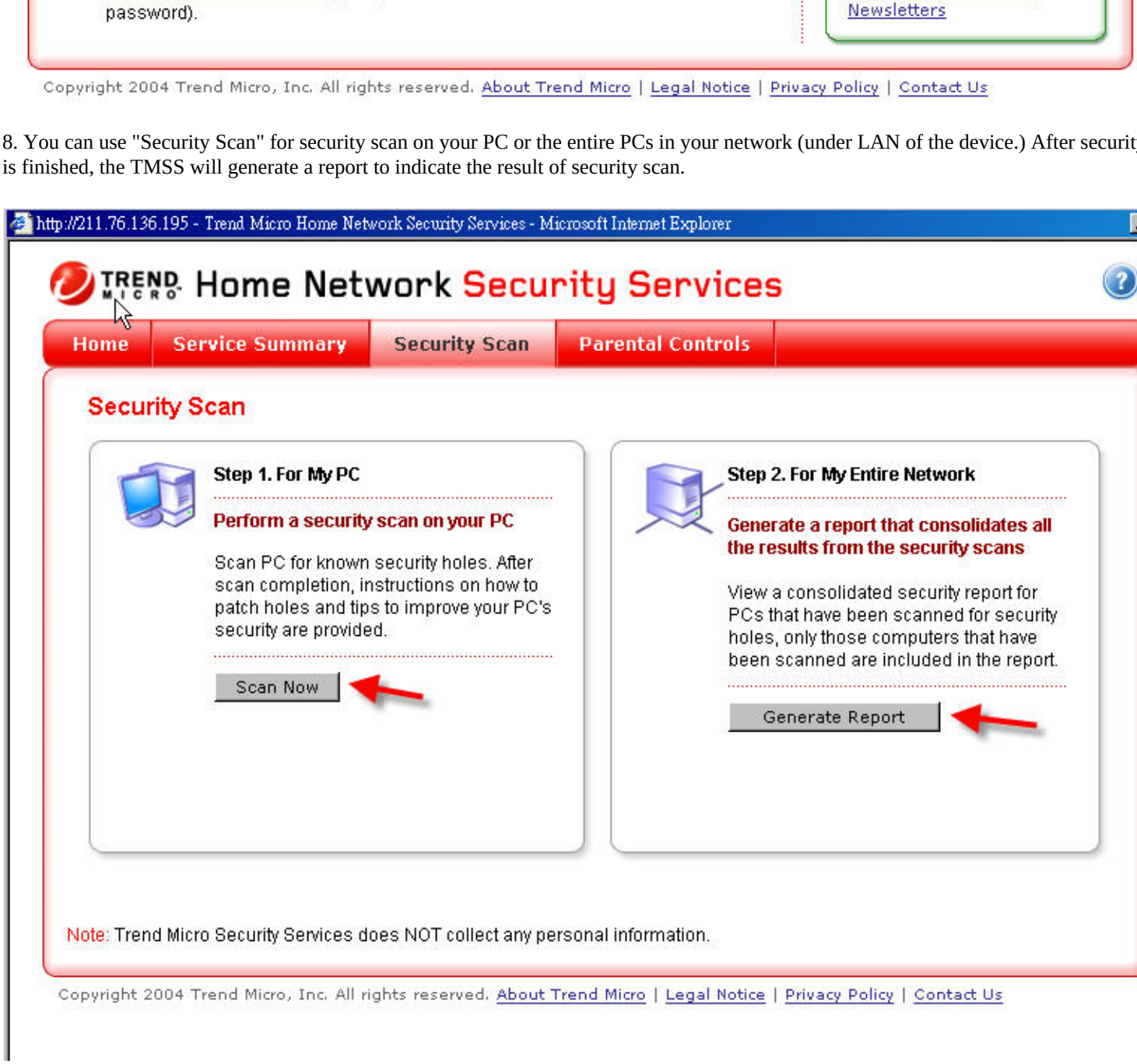


6. After you receive the registration mail from TMSS, please follow the instruction in the mail to validate your account. After you validate your account, you will be redirect to the page below and you can download TIS 60 days trial version. (Trend Micro Internet Security)

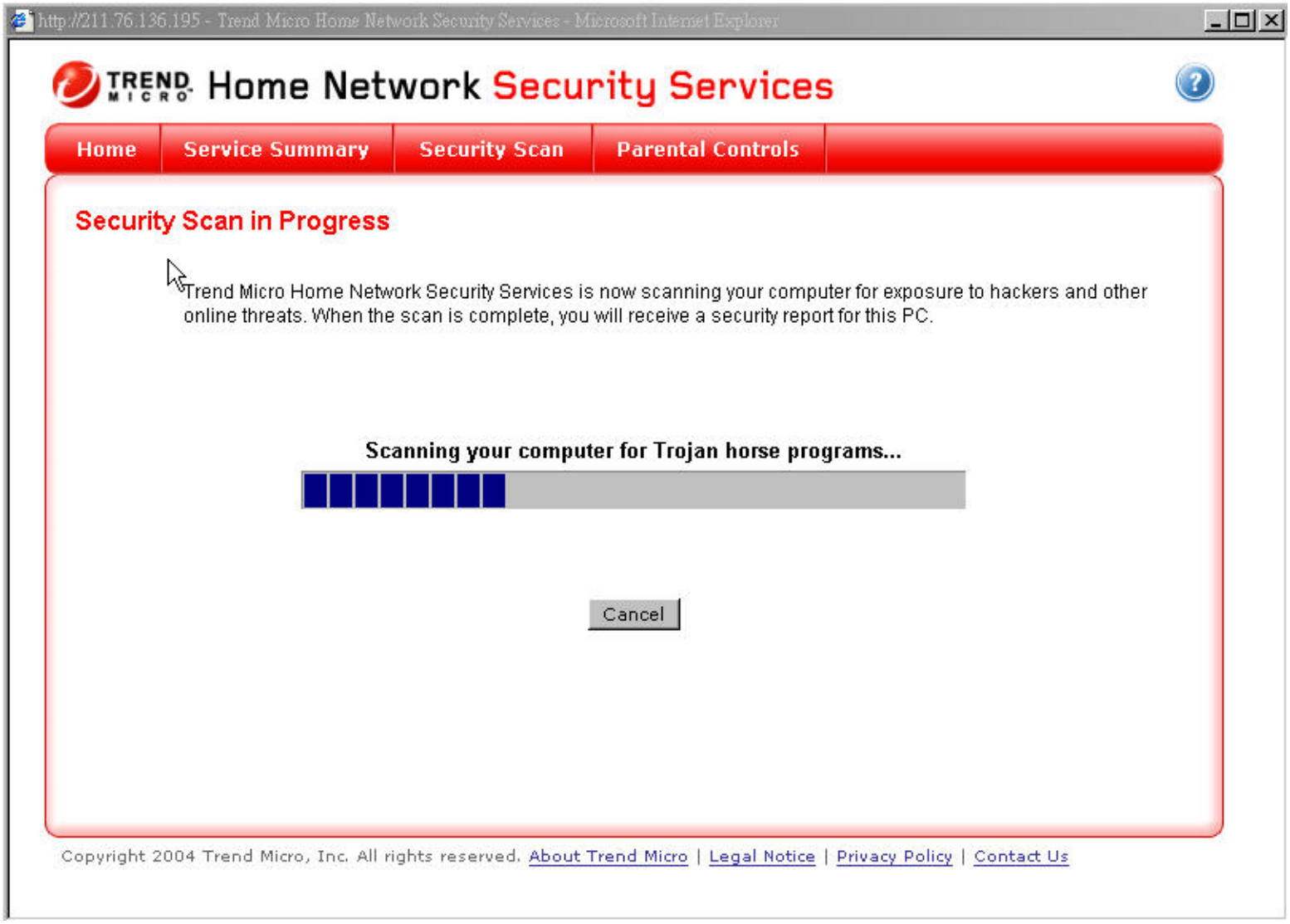


7. You can back to TMSS dashboard, you can see the status already change. (If you want extend you TMSS service after Trial expired, please check the Online Support or press "?" mark for more detail information.)



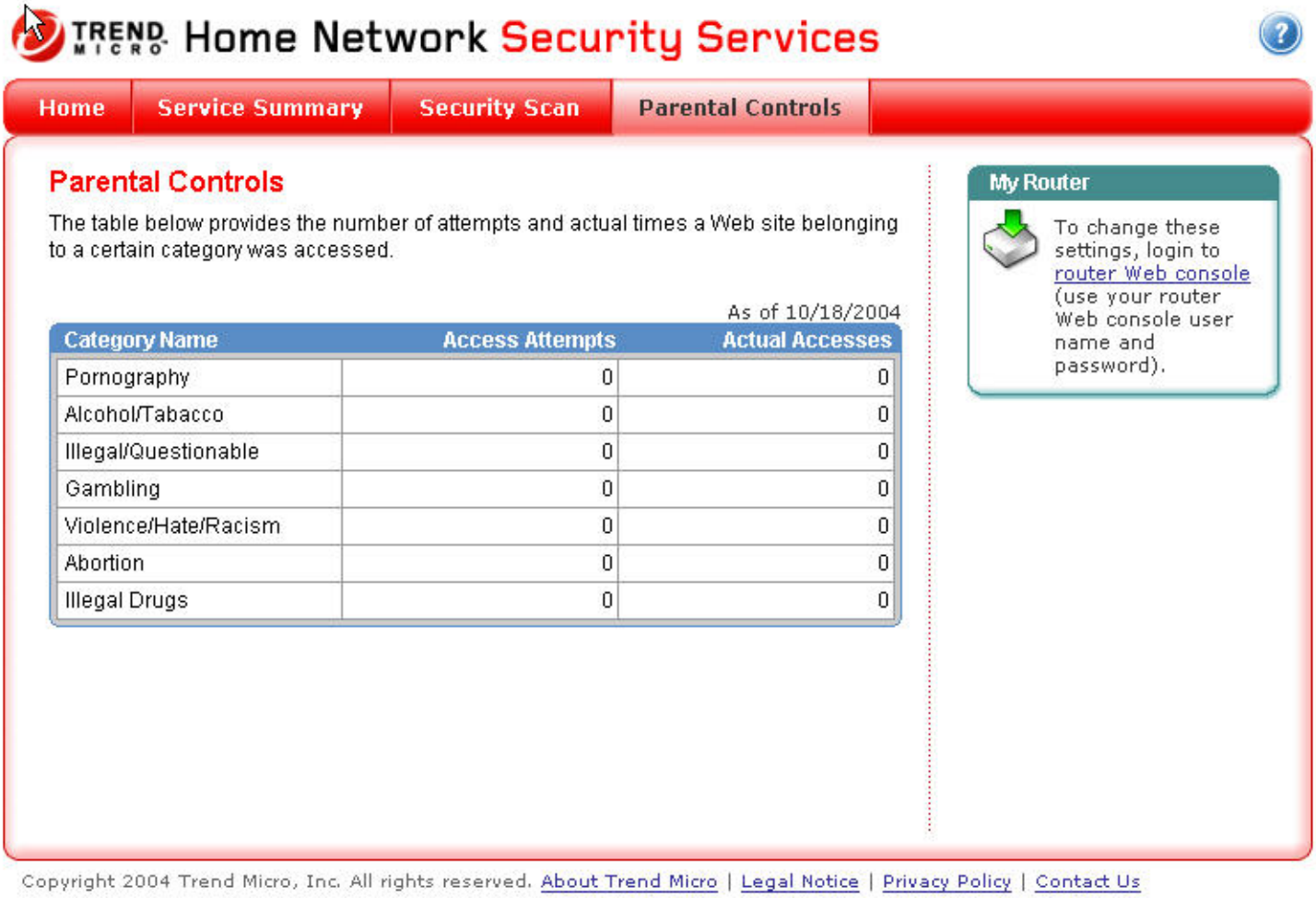


8. You can use "Security Scan" for security scan on your PC or the entire PCs in your network (under LAN of the device.) After security scan is finished, the TMSS will generate a report to indicate the result of security scan.

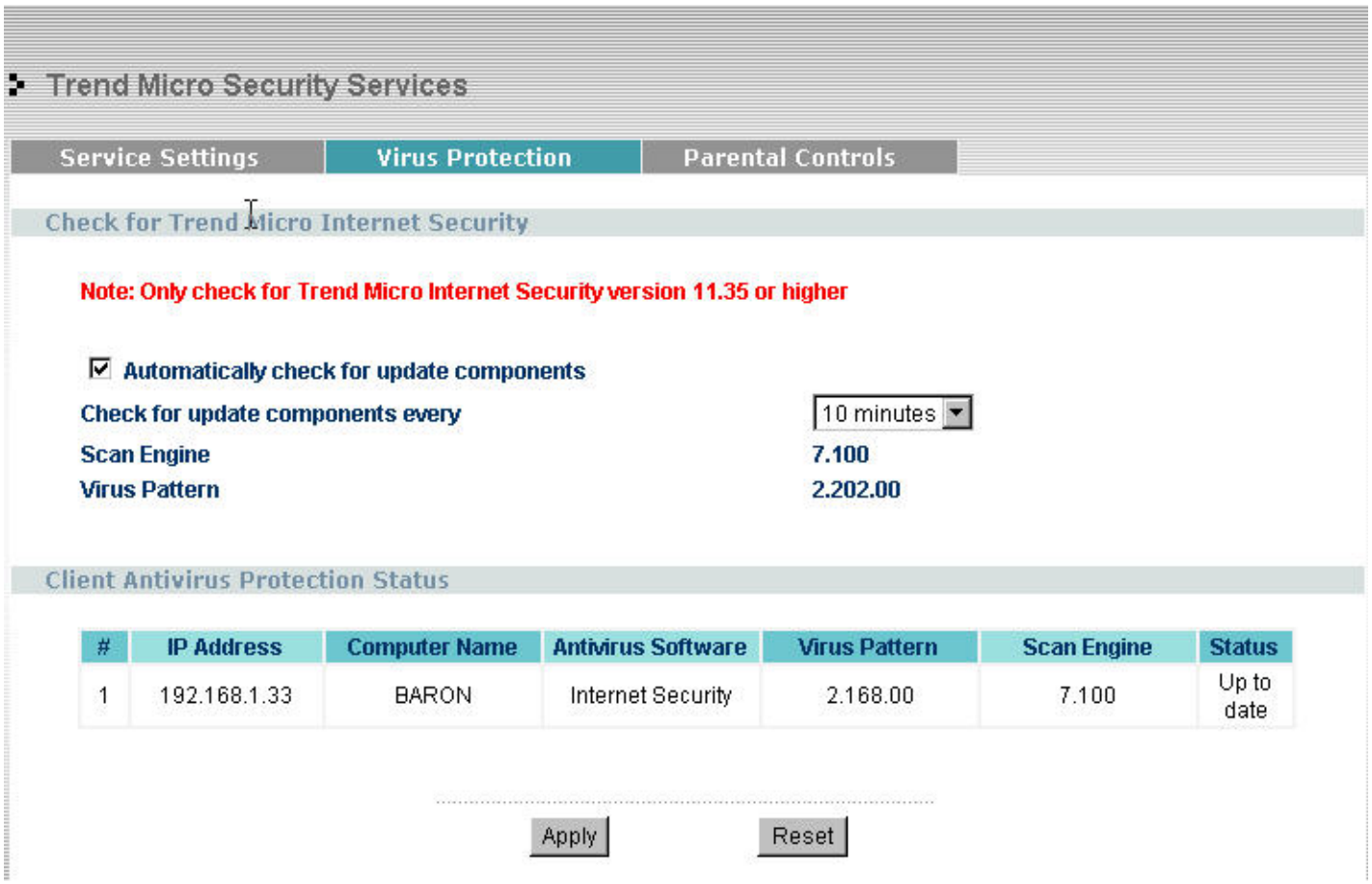


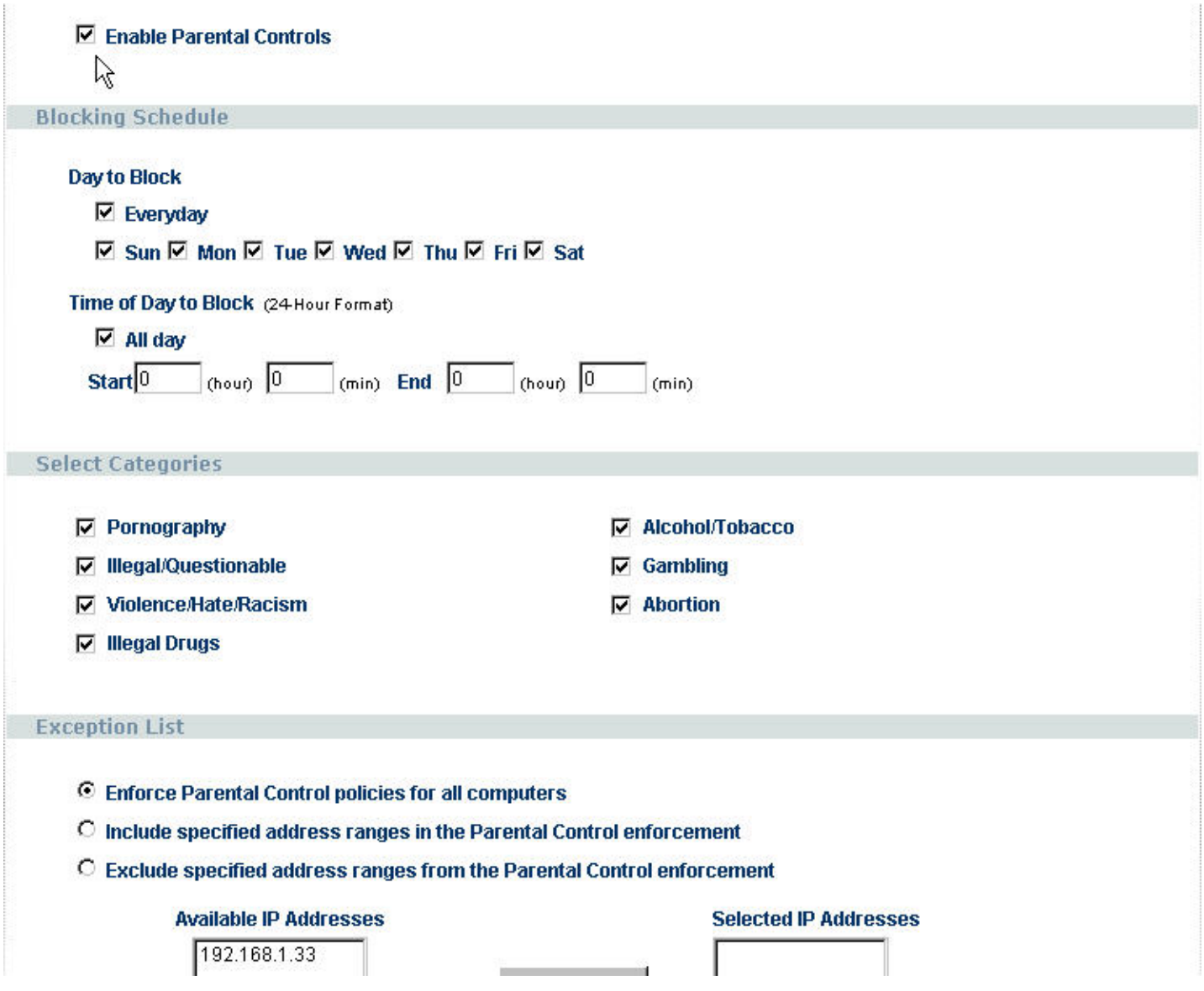
9. Before you validate your account, the status of Parental Control will like below.

10. Below is the page which you validate your account.



11. After you finish your TMSS registration and install the TIS software, in Web GUI will display as below. (the information of Client Antivirus Protection Status and the setting column of Parental Control.)


Trend Micro Security Services
Service Settings
Virus Protection
Parental Controls
Check for Trend Micro Internet Security
Note: Only check for Trend Micro Internet Security version 11.35 or higher
Automatically check for update components
Check for update components every
10 minutes
Scan Engine
7.100
Virus Pattern
2.202.00
Client Antivirus Protection Status
| IP Address | Computer Name | Antivirus Software | Virus Pattern | Scan Engine | Status
1 | 192.168.1.33 | BARON | Internet Security | 2.168.00 | 7.100 | Up to date
Apply
Reset


Enable Parental Controls
Blocking Schedule
Day to Block
Everyday
Sun Mon Tue Wed Thu Fri Sat
Time of Day to Block (24-Hour Format)
All day
Start 0 (hour) 0 (min) End 0 (hour) 0 (min)
Select Categories
Pornography
Illegal/Questionable
Violence/Hate/Racism
Illegal Drugs
Alcohol/Tobacco
Gambling
Abortion
Exception List
Enforce Parental Control policies for all computers
Include specified address ranges in the Parental Control enforcement
Exclude specified address ranges from the Parental Control enforcement
Available IP Addresses
192.168.1.33
Selected IP Addresses

TMSS FAQ

---

1. Entire network result will never be "Risk Free".

If user has TIS installed and updated, the status is "Low Risk"
-> entire network status will never be "Risk Free¡§

2. If user sets incorrect DNS setting for router, parental controls will not work.

Router needs the DNS setting to query ASP server for URL rating.

3. If router's web server does not use port 80, TMSS service will not work.

Reproduce steps :

1. change the port of web server from 80 to 8080 at router's web console (if the router support this function)
2. TMSS service will not work with this router since the expected port 80 does not response

4. The scanning result will be sent to default gateway.

If our network topology is using multiple routers,

e.g. ADSL-----TMSS router------ router2(default gateway)------PC
It will assume that the default gateway is the TMSS router. In hence, data will not go to the true TMSS router.

5. If the client is in exception list but router reboots, web console will not display this client.

Until it has first http traffic via router.

6. Downloading Internet Security (27MB) will cost much time.

When user clicks the "Start Download & Install" button, he has to wait for about 30 minutes with 512kbps ADSL to see the security warning message pops up.

7. VA did not localized into DE and FR.

Now we only have VA XML file in English.

8. If user has proxy, only http(port:80) will be redirected to Dashboard web site.

If user has to setup a proxy to connect to internet, the proxy must use port 80. So TMSS router can redirect to Dashboard web server.

9. When upgrading ActiveX, it prompts to ask user to reboot.

It is caused by IE's behavior that will prompt users to reboot the computer, so that the updated ActiveX Control can be actually installed.

The reboot message is from system. However, New ActiveX Control is still useable. Although users don't reboot, the reboot message will keep prompting until users restart IE or reboot the machine. Users can restart IE to complete the updating process.

10. Strange characters are displayed at detailed scanning result (win98 SE).

Due to the Win9X don't support Unicode, and the tmvainfo.xml use utf8 format to describe the messages.

11. IE 5.0 treats our ActiveX as an expired components.

12. TMSS will not update the client information before DQM time out reaches.

If client installed TIS or updates pattern, TMSS will not get those information into client-info because TMSS will not send DQM to query client status before DQM time(30 mins) out reach.

13. If port 40116(UDP) is used by another program, discovery would be failed.

14. When Box's client table is full, new client is not allowed to access internet.

15. Redirected page will be blocked by google's tool & XP sp2.

Google's tool will block any "pop up" window by default.

Windows XP sp2 will release at 8/04/2004 that it will also block the pop up window TMSS 1.0 introduced.

16. Script error when using IE5 to view other client's report.

No error happens if running IE version 5.5 or later.

17. If user register his name in Chinese , it won't be shown in the verification mail, and become ??? instead.

CI Command List

Command Class List Table		
System Related Command	Exit Command	Device Related Command
Ethernet Related Command	POE Related Command	PPTP Related Command
Configuration Related Command	IP Related Command	IPSec Related Command
Firewall Related Command	Wireless LAN Related Command	Bridge Related Command
Radius Related Command	802.1x Related Command	

To issue the CI commands, you can either use telnet or console connection, and then go to SMT menu 24.8.

Command Syntax and General User Interface

CI has the following command syntax:

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

General user interface:

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

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostname		[hostname]	display system hostname
	logs			
		category		

			access [0:none/1:log/2:alert/3: both]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3: both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display	[access|attack|error|ipsec|ike| javablocked|mten|urlblocked|urlfor ward]	display all logs or specify category logs
		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer
		mail		

			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2: daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2: tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
	log			
		clear		clear log error
		disp		display log error
		online	[on|off]	turn on/off error log online display

		resolve		Resolve mail server and syslog server address
	mbuf			
		link	link	list system mbuf link
		pool	<id> [type]	list system mbuf pool
		status		display system mbuf status
		disp	<address>	display mbuf status
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		debug	[on|off]	
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[minute]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time

	trcdisp			monitor packets
	trclog			
	trcpacket			
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on|off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile
	server			
		access	<telnet|ftp|web|icmp|snmp|dns> <value>	set server access type
		load		load server information
		disp		display server information
		port	<telnet|ftp|web|snmp> <port>	set server port
		save		save server information
		secureip	<telnet|ftp|web|icmp|snmp|dns> <ip>	set server secure ip addr

	fwnotify			
		load		load fwnotify entry from spt
		save		save fwnotify entry to spt
		url	<url>	set fwnotify url
		days	<days>	set fwnotify days
		active	<flag>	turn on/off fwnotify flag
		disp		display firmware notify information
		check		check firmware notify event
		debug	<flag>	turn on/off firmware notify debug flag
	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		netbios		
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable

		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization
	filter			
		netbios		
	upnp			
		active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
		config	[0:deny/1:permit]	Allow users to make configuration changes. through UPnP
		display		display upnp information
		firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.
		load		save upnp information
		save		save upnp information

Command				Description
exit				exit smt menu

Device Related Command Home

Command				Description
dev				
	channel			
		drop	<channel_name>	drop channel
	dial		<node#>	dial to remote node

Ethernet Related Command
Home

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	version			see ethernet device type

	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on|off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
	debug			
		disp	<ch_name>	display ethernet debug infomation
		level	<ch_name> <level>	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		accessblock	<0:disable 1:enable>	block internet access
		save		save ether data to spt

POE Related Command Home

Command				Description
poe				
	status		[ch_name]	see poe status
	dial		<node>	dial a remote node

	drop		<node>	drop a pppoe call
	ether		[rfc|3com]	set /display pppoe ether type

PPTP Related Command Home

Command				Description
pptp				
	dial		<rn-name>	dial a remote node
	drop		<rn-name>	drop a remote node call
	tunnel		<tunnel id>	display pptp tunnel information

Configuration Related Command Home

Command					Description
config					The parameters of config are listed below.
edit	firewall	active <yes|no>			Activate or deactivate the saved firewall settings
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings
display	firewall				Displays all the firewall settings
		set <set#>			Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set.
		set <set#>	rule <rule#>		Display current entries of a rule in a set.

		attack			Display all the attack alert settings in PNC
		e-mail			Display all the e-mail settings in PNC
		?			Display all the available sub commands
		e-mail	mail-server <mail server IP>		Edit the mail server IP to send the alert
			return-addr <e-mail address>		Edit the mail address for returning an email alert
			e-mail-to <e-mail address>		Edit the mail address to send the alert
			policy <full | hourly |daily | weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes| no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes|no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold

			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incomplete <0~255>		The threshold to start executing the block field
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward| block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated

			pnc <yes|no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes|no>		Switch on/off sending the log for matching the default permit
			rule <rule#>	permit <forward|block>	Edit whether a packet is dropped or allowed when it matches this rule
				active <yes|no>	Edit whether a rule is enabled or not
				protocol <0~255>	Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				log <none|match|not-match|both>	Sending a log for a rule when the packet none|matches|not match|both the rule
				alert <yes|no>	Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Select and edit a source address of a packet which complies to this rule
				srcaddr-subnet <ip address> <subnet mask>	Select and edit a source address and subnet mask if a packet which complies to this rule.
				srcaddr-range <start ip address> <end ip address>	Select and edit a source address range of a packet which complies to this rule.
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.

				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired custom port name
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1|0>				Turn on|off trace for firewall debug information.

IP Related Command

Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		server	<primary> [secondary] [third]	set dns server
		stats		
			clear	clear dns statistics
			disp	display dns statistics
	httpd			
	icmp			

		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	smtp			
	status			display ip statistic counters
	stroute			
		display	[rule # | buf]	display rule index or detail message in rule.
		load	<rule #>	load static route rule in buffer
		save		save rule from buffer to spt.
		config		
			name <site name>	set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]	set static route destination address and gateway.

			mask <IP subnet mask>	set static route subnet mask.
			gateway <IP address>	set static route gateway address.
			metric <metric #>	set static route metric number.
			private <yes|no>	set private mode.
			active <yes|no>	set static route rule enable or disable.
	traceroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	ave			anti-virus enforce
	urlfilter			
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature

			logAndBlock [log/ logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh: mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/ disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags

			logFlags [type(1-3)][enable/ disable]	set log flags
			add [string] [trust/untrust/ keyword]	add url string
			delete [string] [trust/untrust/ keyword]	delete url string
			clearAll	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	nat			
		server		

			disp	display nat server table
			load <set id>	load nat server information from ROM
			save	save nat server information to ROM
			clear <set id>	clear nat server information
			edit active <yes|no>	set nat server edit active flag
			edit svrport <start port> [end port]	set nat server server port
			edit intport <start port> [end port]	set nat server forward port
			edit remotehost <start ip> [end ip]	set nat server remote host ip
			edit leasetime [time]	set nat server lease time
			edit rulename [name]	set nat server rule name
			edit forwardip [ip]	set nat server server ip
			edit protocol [protocol id]	set nat server protocol
			edit clear	clear one rule in the set
		service		
			irc [on|off]	turn on/off irc flag
		resetport		reset all nat server table entries
		incikeport	[on|off]	turn on/off increase ike port flag
	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on|off]	turn on/off igmp forward to all interfaces flag

		querier	[on|off]	turn on/off igmp stop query flag
		iface		
			<iface> grouptm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold
			<iface> v1compat [on|off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status
	pr			

IPSec Related Command Home

Command				Description
ipsec				
	debug	<1|0>		turn on|off trace for IPsec debug information
	ipsec_log_disp			show IPSec log, same as menu 27.3

	route	lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it.

				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES +MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.

		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group
		name	<string>	Set rule name
		name	<string>	Set rule name
		keeyAlive	<Yes| No>	Set keep alive or not
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address
		peerIdType	<0:IP | 1:DNS | 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address | Domain name>	Set secure gateway address or domain name
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port

		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		antiReplay	<Yes | No>	Set anitreplay or not
		keyManage	<0:IKE | 1:Manual>	Set key manage
		ike	negotiationMode <0:Main | 1: Aggressive>	Set negotiation mode in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			p1EncryAlgo <0:DES | 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 | 1: SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 | 1: DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH | 1: ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 | 1: SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
			encap <0:Tunnel | 1: Transport>	set encapsulation in phase 2 in IKE

			pfs <0:None | 1:DH1 | 2: DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH | 1: ESP>	Set active protocol in manual
		manual ah	encap <0:Tunnel | 1: Transport>	Set encapsulation in ah in manual
			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		manual esp	encap <0:Tunnel | 1: Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual

Firewall Related Command Home

Command				Description
sys	Firewall			
		acl		
			disp	Display specific ACL set # rule #, or all ACLs.

		active	<yes|no>	Active firewall or deactivate firewall
		clear		Clear firewall log
		cnt		
			disp	Display firewall log type and count.
			clear	Clear firewall log count.
		disp		Display firewall log
		online		Set firewall log online.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		update		Update firewall
		dynamicrule		
		tcprst		
			rst	Set TCP reset sending on/off.
			rst113	Set TCP reset sending for port 113 on/off.
			display	Display TCP reset sending setting.
		icmp		
		dos		
			smtp	Set SMTP DoS defender on/off
			display	Display SMTP DoS defender setting.
			ignore	Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore		
			dos	Set if firewall ignore DoS in lan/wan/dmz/wlan

			triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan

Wireless LAN Related Command Home

Command				Description
wlan				
	active		[on|off]	set on/off wlan
	association			display association list
	chid		[channel id]	set channel
	diagnose			self-diagnostics
	essid		[ess id]	set ESS ID
	version			display WLAN version information

Bridge Related Command

Command				Description
Bridge				
	cnt			related to bridge routing statistic table
		Disp		display bridge route counter
		Clear		clear bridge route counter
	stat			related to bridge packet statistic table
		Disp		display bridge route packet counter

		Clear		clear bridge route packet counter

Radius Related Command

Command				Description
Radius				
	auth			show current radius authentication server configuration
	acct			show current radius accounting server configuration

802.1x Related Command

Command				Description
8021x				
	debug	Level	[debug level]	set ieee802.1x debug message level
		Trace		show all supplications in the supplication table
		User	[username]	show the specified user status in the supplicant table

Prestige 334WT Troubleshooting

My P334WT can not get an IP address from the ISP to connect to the Internet, what can I do?

Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use three ways:

1. Check if the 'MAC address' is valid
2. Check if the 'Host Name' is valid, e.g., @home
3. Check if the 'User ID' is valid, e.g., RR-Toshiba Authentication Service, RR-Manager Authentication Service

If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

---

1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for authentication. So, if a new network card is used or the P334WT is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP.

The problem can be simply solved if the ISP allows you to use a new MAC, and you just tell them the WAN MAC of the P334WT. The WAN MAC of the P334WT can be obtained from menu 24.1.

In case the ISP does not allow you to use a new MAC, the P334WT can clone the MAC from the first PC you installed as the WAN MAC and send it to the ISP. To clone the MAC from the PC you need to enter that PC's IP in menu 2. Once the MAC is received by the P334WT, the WAN MAC in menu 24.1 will be updated.

```
                    Menu 2 - WAN Setup

                    Link Mode= Half Duplex

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

¡@
```

Key settings:

- Assigned By=, Choose **'IP address attached on LAN'**.
- IP Address=, Enter the IP address of the PC which is installed by the ISP at the first installation.

¡@

---

2. Your ISP checks the 'Host Name'

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. When first installing, the ISP's tech people configure the host name as the 'Computer Name' of the PC in the 'Networking' settings. When the P334WT is attached to the cable modem to connect to the ISP, we should configure this host name in the P334WT's system (menu 1).

```
    ¡@

        Menu 1 - General Setup

        System Name= zyxel
```

Key Setting:

- System Name=, The system name must be the same as the PC's computer name.

¡@

---

3. Your ISP checks 'User ID'

This authentication type is used by RoadRunner ISP, currently they use RR-TAS(Toshiba Authentication Service) and RR-Manager authentications. You must configure the correct 'Service Type', username and password for your ISP in menu 4.

```
¡@

     Menu 4 - Internet Access Setup

     ISP's Name= ChangeMe
     Service Type= RR-Toshiba Authentication Service
     Server IP= 0.0.0.0
     My Login=
     My Password= ********

     IP Address Assignment= Dynamic
     IP Address= N/A
     IP Subnet Mask= N/A
     Gateway IP Address= N/A
     RIP Direction= None
     Version= N/A
     Single User Account= Yes
     Edit Filter Set= No


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

Key settings:

- Service Type.....Currently, there are two authentication types that Road Runner supports, **RR-TAS** and **RR-Manager.** Choose the correct one for your local ISP.
- Server IP.....The P334WT will find the Road Runner server IP if this field is blank, otherwise enter the authentication server IP address if you know it.
- My Login Name...Enter the login name given to you by your ISP
- My Password.....Enter the password associated with the login name
- WAN IP Address Assignment...If the ISP did not assign you an explicit IP, select **Dynamic**, otherwise, select **Static**.
- IP Address & Subnet Mask & Gateway IP Address...Enter the IP address, subnet mask & gateway IP when **Static** Assignment is selected above.

If any application does not work behind P334WT's SUA

1. Currently, the applications supported in SUA mode are listed in the ZyXEL SUA Support Table. Please check all the required settings suggested in the table to configure your P334WT.
2. If your application is not in the table or it is in the table but still does not work, please configure the workstation which runs the applications as the SUA default server in SMT 15 and try again.
3. If it still does not work then please provide the application name, version and the following trace for our analysis.

```
P324>ip sua ifa enif1
```

Embedded Packet Trace

The P334WT 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 P334WT. 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:`

```
P324> sys trcp channel enet1 none
P324> sys trcp channel enet0 bothway
P324> sys trcp sw on
P324> sys trcl sw on
P324> sys trcd brief
   0    11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   1    11883.100 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   2    11883.330 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1108
   3    11883.340 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   4    11883.340 ENET0-R[0339] TCP 192.168.1.2:1108->192.31.7.130:80
   5    11883.610 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   6    11883.620 ENET0-T[0102] TCP 192.31.7.130:80->192.168.1.2:1108
   7    11883.630 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   8    11883.630 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   9    11883.650 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  10    11883.650 ENET0-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80
P324> sys trcd parse
---
<0000>-------------------------------------------------------------
LAN Frame: ENET0-RECV   Size:  62/  62   Time: 12089.790 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

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

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

  TCP Header:
    Source Port              = 0x045C (1116)
    Destination Port         = 0x0050 (80)
    Sequence Number          = 0x00BD15A7 (12391847)
    Ack Number               = 0x00000000 (0)
    Header Length            = 28
```

```
    Flags                    = 0x02 (....S.)
    Window Size              = 0x2000 (8192)
    Checksum                 = 0xBEC3 (48835)
    Urgent Ptr               = 0x0000 (0)
    Options                  =
        0000: 02 04 05 B4 01 01 04 02

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

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

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

  TCP Header:
    Source Port              = 0x0050 (80)
    Destination Port         = 0x045C (1116)
    Sequence Number          = 0x4AD1B57F (1255257471)
    Ack Number               = 0x00BD15A8 (12391848)
    Header Length            = 24
    Flags                    = 0x12 (.A..S.)
```

```
    Window Size               = 0xFAF0 (64240)
    Checksum                  = 0xF877 (63607)
    Urgent Ptr                = 0x0000 (0)
    Options                   =
        0000: 02 04 05 B4

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

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

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

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

```
    Urgent Ptr                = 0x0000 (0)

  TCP Data: (Length=6, Captured=6)
    0000: 20 20 20 20 20 20

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

2. Trace WAN packet

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:

```
P324> sys trcp channel enet0 none
P324> sys trcp channel enet1 bothway
P324> sys trcp sw on
P324> sys trcl sw on
P324> 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
P324> 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)
    Idetification            = 0xB139 (45369)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0xEE (238)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0xA9AB (43435)
    Source IP                = 0xC01F0782 (192.31.7.130)
    Destination IP           = 0xCA849B61 (202.132.155.97)

  TCP Header:
    Source Port              = 0x0050 (80)
    Destination Port         = 0x281E (10270)
    Sequence Number          = 0xD3E95985 (3555285381)
    Ack Number               = 0x00C18F63 (12685155)
    Header Length            = 20
    Flags                    = 0x19 (.AP..F)
    Window Size              = 0xFAF0 (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)
    Idetification            = 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)
    Idetification            = 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...
P324>
```

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 P334WT 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>**

Exmaple:

```
P324> sys trcp channel enet1 none
P324> sys trcp channel enet0 bothway
P324> sys trcp sw on
P324> sys trcl sw on
P324> sys trcp sw off
P324> sys trcl sw off
P324> sys trcp brief
   0    10855.790 ENET0-T[0141] TCP 192.31.7.130:80->192.168.1.2:1102
   1    10855.800 ENET0-R[0060] TCP 192.168.1.2:1102->192.31.7.130:80
   2    10855.810 ENET0-R[0062] TCP 192.168.1.2:1103->192.31.7.130:80
   3    10855.840 ENET0-R[0062] TCP 192.168.1.2:1104->192.31.7.130:80
   4    10856.020 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1102
   5    10856.030 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1103

   6    10856.040 ENET0-R[0060] TCP 192.168.1.2:1103->192.31.7.130:80
P324> sys trcp parse 5 5
---
<0005>-----------------------------------------------------------------
LAN Frame: ENET0-XMIT   Size:  58/  58   Time: 10856.030 sec
Frame Type: TCP 192.31.7.130:80->192.168.1.2:1103

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

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x002C (44)
    Idetification            = 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                    ..........
P324>
```

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 P334WT 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:

```
P324> sys trcp channel enet0 none
P324> sys trcp channel enet1 bothway
P324> sys trcl sw on
P324> sys trcp sw on
P324> sys trcl sw off
P324> sys trcp sw off
P324> 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
P324> 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)
    Idetification            = 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)
    Idetification            = 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
P324>
¡@
```

Debug PPPoE Connection

The P334WT 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 P334WT
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 P334WT crashes and you can do nothing, please send the above log back to us.
6. If the P334WT 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 P334WT 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
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
bdcastSendInit: l1.pktTx() failed, pch poe0 ch enet0
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
```

```
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0.........
poeI/C: ver 1 type 1 code x07 sessId x0000 len 274(x0112)
poeCtrlI/C: pkt len 274
poeGetTags()
service-name
service-name telstra
service-name bpa
service-name iprimus
service-name pacificinternet
service-name integrationisp
service-name bpa-dev
service-name bpa-sif
service-name telstrarna
service-name gpmsystems
service-name cmux
service-name launceston-broadband
service-name vivanet
service-name n1234567k00
service-name bigpond
service-name n7061992k
service-name n3068223k
service-name n2155202k
service-name n7061995k
AC-name vet1-exhibition-bsn-1
host-uniq 31303030 len 4
PADO recv'd, chann enet1
procPADO: for poe chann poe0
Chann poe0 sending request
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x19 sess-id 0 len 12(x000C)
Undefined Address : 0xE3F045C4
Undefined Data : 0x56FF54FF
    r0= 0xE3F045C4    r1= 0x0001FFC0    r2= 0x000000E5    r3=
0x56FF54FF
    r4= 0xE3F045C4    r5= 0xE5BDBFEC    r6= 0x0001C468    r7=
0x60000093
    r8= 0x00000000    r9= 0xE3550000     r10=0xE3550000    fp=
0x00000000
    r12=0x56FF54FF    sp= 0x0001EDBC    lr= 0x00004F64    pc=
0x00013954
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
e5bdbfe0: e2 8f 00 06 e5 d5 20 06 e5 d5 20 0a e5 d5 20 0e ...b...
f...j...n
```

```
e5bdbff0: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc000: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc010: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc020: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc030: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc040: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc050: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc060: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc070: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc080: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc090: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc0a0: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc0b0: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc0c0: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc0d0: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
e5bdc0e0: 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...
f...j...n
Bootbase Version: V1.12 | 1/27/2000 11:00:09
RAM: Size = 4096 Kbytes
FLASH: Intel 8M
RAS Version: V3.20(M.01)b2 | 8/18/2000 14:05:08

Enter Debug Mode
atgo
Bootbase Version: V1.12 | 1/27/2000 11:00:09
RAM: Size = 4096 Kbytes
FLASH: Intel 8M
RAS Version: V3.20(M.01)b2 | 8/18/2000 14:05:08

Press any key to enter debug mode within 3 seconds.
.....................................................
```

```
initialize ch =0, ethernet address: 00:a0:c5:e1:ee:d8
initialize ch =1, ethernet address: 00:a0:c5:e1:ee:d9
Press ENTER to continue...

                  Enter Password : XXXX
```