# P-661H-D Series

ADSL2+ 4-port Security Gateway

# Support Notes

Version3.40
Mar. 2006

# FAQ

## 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. What's Multilingual Embedded Web Configurator?

Multilinggual Embedded Web Configurator means that it can display with 3 kinds of languanges: English, French, and German. By factory default it displays with English, and you can change it in Web GUI.

### 3. How do I access the P-661H-D Command Line Interface (CLI)?

The Command Line Interface is for the Administrator use only, and it could be accessed via telnet session.
**Note: It is protected by super password, '1234' by factory default.**

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

You can do this if you access the P-661H-D as Administrator. You can upload the firmware and configuration file to Prestige from Web Condigurator, or using FTP or TFTP client software. You CAN NOT upload the firmware and configuration file via Telnet because the Telnet connection will be dropped during uploading the firmware. Please do not power off the router right after the FTP or TFTP uploading is finished, the router will upload the firmware to its flash at this moment.
**Note: There may be firmware that could not be upgraded from Web Configurator. In this case, ZyXEL will prepare special Upload Software for you. Please read the firmware release note carefully when you want to upload a new fireware.**

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

The P-661H-D allows you to transfer the firmware to P-661H-D 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 P-661H-D.

b. Enter CI command **'sys stdio 0'** to disable Stdio 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 P-661H-D 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 restore P-661H-D configurations by using TFTP client program via LAN?**

a. Use the TELNET client program in your PC to login to your P-661H-D.
b. Enter CI command **'sys stdio 0'** disable Stdio idle timeout
c. To backup the P-661H-D configurations, use TFTP client program to get file **'rom-0'** from the P-661H-D.
d. To restore the P-661H-D configurations, use the TFTP client program to put your configuration in file **rom-0** in the P-661H-D.

**7. What should I do if I forget the system password?**

In case you forget the system password, you can erase the current configuration and restore factory defaults this way:

Use the **RESET button** on the rear panel of P-661H-D to reset the router. After the router is reset, the LAN IP address will be reset to **'192.168.1.1',** the common user password will be reset to **'user',** the Administrator password will be reset to '**1234'.**

**8. How to use the Reset button?**

a. Turn your P-661H-D on. Make sure the **POWER** led is on (not blinking)
b. Press the **RESET** button for longer than one second and shorter than five seconds and release it. If the **POWER** LED begins to blink, the P-661H-D's wireless auto security function-**OTIST** has been enabled.
c. Press the **RESET** button for six seconds and release it. If the **POWER** LED begins to blink, the default configuration have been restored and the P-661H-D restarts.

**9. 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.

**10. What is the difference between SUA and Full Feature NAT?**

When you edit a remote node in Web Configurator, Advanced Setup, **Network -> Remote Node -> Edit,** there will be three options for you:

- **None**
- **SUA Only**
- **Full Feature**

**SUA** (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules: **Many-to-One** and **Server**. With SUA, 'visible' servers had to be mapped to different ports, since the servers share only one global IP.

The P-661H-D now has **Full Feature NAT** which supports five types of IP/Port mapping: One to One, Many to One, Many to Many Overload, Many to Many No Overload and Server. You can make special application when you select **Full Feature NAT**. For example: With multiple global IP addresses, multiple severs using the same port (e.g., FTP servers using port 21/20) are allowed on the LAN for outside access.

The P-661H-D supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The P-661H-D supports 8 sets since there are 8 remote nodes.

By fatory default, the NAT is select as **SUA** in Web Configurator, Advanced Setup, **Network -> NAT -> General -> NAT Setup.**

**11. Is it possible to access a server running behind SUA from the outside Internet? How can I do it?**

Yes, it is possible because P-661H-D 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. (You can configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding**).

### 12. When do I need select Full Feature NAT?

- Make multiple local servers on the LAN accessible from outside with multiple global IP addresses

With SUA, 'visible' servers had to be mapped to different ports, since the servers share only one global IP. But when you select **Full Feature**, you can make multiple local servers (mapping the same port or not) on the LAN accessible from outside with multiple global IP addresses.

- 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.

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

Multi-NAT supports five types of IP/port mapping: 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),

- **One to One**: In One-to-One mode, the P-661H-D maps one ILA to one IGA.
- **Many to One:** In Many-to-One mode, the P-661H-D 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 is optional in today's Prestige routers).
- **Many to Many Overload:** In Many-to-Many Overload mode, the P-661H-D maps the multiple ILA to shared IGA.
- **Many One-to-One:** In Many One-to-One mode, the P-661H-D maps each ILA to unique IGA.
- **Server:** In Server mode, the P-661H-D 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 the five types.

| NAT Type | IP Mapping |
|---|---|
| One-to-One | ILA1<--->IGA1 |
| Many-to-One (SUA/PAT) | ILA1<--->IGA1<br>ILA2<--->IGA1<br>... |
| Many-to-Many Overload | ILA1<--->IGA1<br>ILA2<--->IGA2<br>ILA3<--->IGA1<br>ILA4<--->IGA2<br>... |
| Many One-to-One | ILA1<--->IGA1<br>ILA2<--->IGA2<br>ILA3<--->IGA3<br>ILA4<--->IGA4<br>... |
| Server | Server 1 IP<--->IGA1<br>Server 2 IP<--->IGA1 |

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

The Prestige does not limit the number of the users but the number of the sessions. The P-661H-D supports 1024 sessions that you can use the **'ip nat session'** command in **CLI** to see. You can also use '**ip nat hashTable wanif0**' to view the current active NAT sessions.

**15. 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'. You can configure the filter rule in **CLI**.

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

**16. How can I protect against IP spoofing attacks?**

The P-661H-D's filter sets provide a means to protect against IP spoofing attacks. The basic scheme is as follows:

For the input data filter:

- Deny packets from the outside that claim to be from the inside

- Allow everything that is not spoofing us

Filter rule setup:

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

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

For the output data filters:

- Deny bounce back 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

### 1. How can I manage P-661H-D?

- Multilingual Embedded Web GUI for Local and Remote management
- CLI (Command-line interface)
- Telnet support (Administrator Password Protected ) for remote configuration change and status monitoring
- FTP/ TFTP sever, firmware upgrade and configuration backup and restore are supported(Administrator Password Protected)

### 2. What is the default password for Web Configurator?

There are two different accounts for P-661H-D Web Configurator: **Common User Account** and **Administrator Account.**
By factory default the password for the two accounts are:

- Common User Account: **user**
- Administrator Account: **1234**.

You can change the password after you logging in the Web Configurator.
**Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.**

### 3. What's the difference between 'Common User Account' and 'Administrator Account'?

For Common User Account, it can only access the status monitor of P-661H-D and check the current system status.

For Administrator Account, besides accessing the status monitor of P-661H-D, it can also access Winzard setup/ Advanced setup of P-661H-D:

Moreover, only with Administrator Password, you could manage the P-661H-D via FTP/TFTP or Telnet.

### 4. How do I know the P-661H-D's WAN IP address assigned by the ISP?

You can view **"My WAN IP <from ISP> : x.x.x.x"** shown in Web Configurator 'Status->Device Information ->WAN Information' to check this IP address.

### 5. What is the micro filter or splitter used for?

Generally, the voice band uses the lower frequency ranging from 0 to 4KHz, while ADSL data transmission uses the higher frequency. The micro filter acts as a low-pass filter for your telephone set to ensure that ADSL transmissions

do not interfere with your voice transmissions. For the details about how to connect the micro filter please refer to the user's manual.

**6. The P-661H-D supports Bridge and Router mode, what's the difference between them?**

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

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

**7. How do I know I am using PPPoE?**

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the P-661H-D if the ISP uses PPPoE.

**8. 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.

**9. What is DDNS?**

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

Without DDNS, we always tell the users to use the WAN IP of the P-661H-D to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-661H-D, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server.

The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-661H-D.

When the ISP assigns the P-661H-D a new IP, the P-661H-D 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.

**10. When do I need DDNS service?**

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the P-661H-D sends this IP to the DDNS server for its updates.

**11. What is DDNS wildcard? Does the P-661H-D support DDNS wildcard?**

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

Yes, the P-661H-D supports DDNS wildcard that http://www.dyndns.org/ supports. When using wildcard, you simply enter yourhost.dyndns.org in the Host field in Menu 1.1 Configure Dynamic DNS.

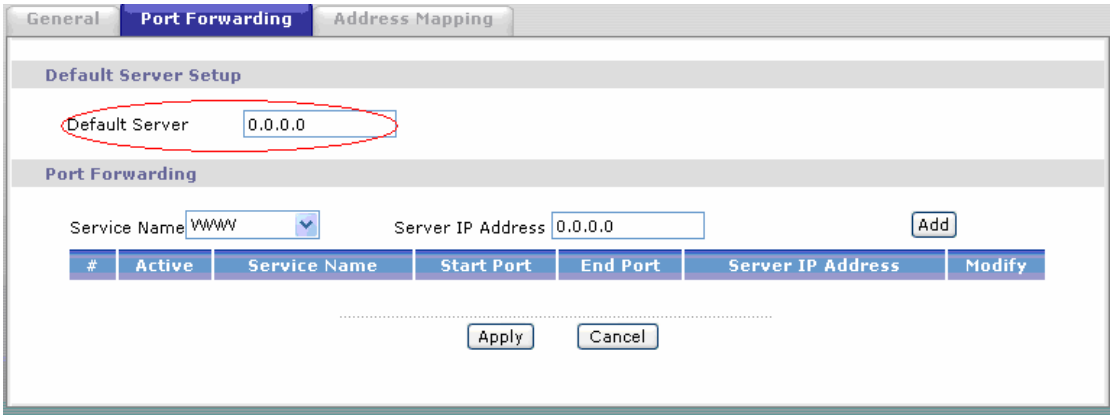
**12. Can the P-661H-D's SUA handle IPSec packets sent by the IPSec gateway?**

Yes, the P-661H-D'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.

**13. How do I setup my P-661H-D 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 is required. You could configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding -> Default Server Setup:**




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 Web configurator. Thus SUA is able to forward the incoming packets to the requested service behind SUA and the outside users access the server using the P-661H-D's WAN IP address. So, we have to configure the internal IPsec client as a default server (unspecified service port) when it acts a server gateway.

### 14. What is Traffic Shaping?

Traffic Shaping allocates the bandwidth to WAN dynamically and aims at boosting the efficiency of the bandwidth. If there are serveral VCs in the P-661H-D but only one VC activated at one time, the P-661H-D allocates all the Bandwidth to the VC and the VC gets full bandwidth. If another VCs are activated later, the bandwidth is yield to other VCs after ward.

### 15. Why do we perform traffic shaping in the P-661H-D?

The P-661H-D must manage traffic fairly and provide bandwidth allocation for different sorts of applications, such as voice, video, and data. All applications have their own natural bit rate. Large data transactions have a fluctuating natural bit rate. The P-661H-D is able to support variable traffic among different virtual connections. Certain traffic may be discarded if the virtual connection experiences congestion. Traffic shaping defines a set of actions taken by the P-661H-D to avoid congestion; traffic shaping takes measures to adapt to unpredictable fluctuations in traffic flows and other problems among virtual connections.

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

Traffic shaping parameters (**PCR, SCR, MBS**) can be set in Web Configurator, Advanced Setup, **Network -> Remote Node -> Edit -> ATM Setup**:

**Peak Cell Rate(PCR):** The maximum bandwidth allocated to this connection. The VC connection throughput is limited by PCR.
**Sustainable Cell Rate(SCR):** The least guaranteed bandwidth of a VC. When there are multi-VCs on the same line, the VC throughput is guaranteed by SCR.
**Maximum Burst Size(MBS):** The amount of cells transmitted through this VC at the Peak Cell Rate before yielding to other VCs. Total bandwidth of the line is dedicated to single VC if there is only one VC on the line. However, as the other VC asking the bandwidth, the MBS defines the maximum number of cells transmitted via this VC with Peak Cell rate before yielding to other VCs.

The P-661H-D holds the parameters for shaping the traffic among its virtual channels. If you do not need traffic shaping, please set SCR = 0, MBS = 0 and PCR as the maximum value according to the line rate (for example, 2.3 Mbps line rate will result PCR as 5424 cell/sec.)

## 17. What do the ATM QoS Types (CBR, UBR, VBR-nRT, VBR-RT) mean?

**Constant bit rate(CBR)**: An ATM bandwidth-allocation service that requires the user to determine a fixed bandwidth requirement at the time the connection is set up so that the data can be sent in a steady stream. CBR service is often used when transmitting fixed-rate uncompressed video.

**Unspecified bit rate(UBR)**: An ATM bandwidth-allocation service that does not guarantee any throughput levels and uses only available bandwidth. UBR is often used when transmitting data that can tolerate delays, such as e-mail.

**Variable bit rate(VBR)**: An ATM bandwidth-allocation service that allows users to specify a throughput capacity (i.e., a peak rate) and a sustained rate but data is not sent evenly. You can select VBR for bursty traffic and bandwidth sharing with other applications. It contains two subclasses:

**Variable bit rate nonreal time (VBR-nRT)**:
**Variable bit rate real time (VBR-RT)**:

## 18. What is content filter?

Internet Content filter allows you to create and enforce Internet access policies tailored to your needs. Content filter gives you the ability to block web sites that contain key words (that you specify) in the URL. You can set a schedule for

when the P-661H-D performs content filtering. You can also specify trusted IP Addresses on LAN for which the P-661H-D will not perform content filtering. You can configure the details about it in Web Configurator, Advanced setup, **Security -> Content Filter.**

# ADSL FAQ

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

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

### 2. What is the expected throughput?

In our test, we can get about 1.6Mbps data rate on 15Kft using the 26AWG loop. The shorter the loop, the better the throughput is.

### 3. What is the microfilter used for?

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

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

You can see the DSL LED Green on the P-661H-D's front panel is on when the ADSL physical layer is up.

### 5. How does the P-661H-D work on a noisy ADSL?

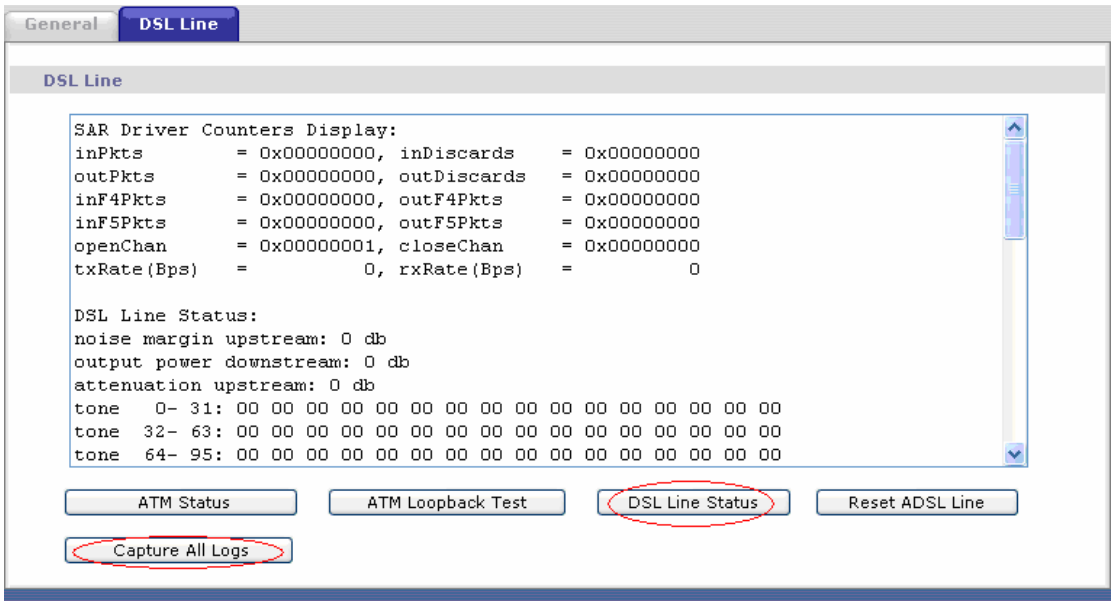
Depending on the line quality, the P-661H-D uses "Fall Back" and "Fall Forward" to automatically adjust the date rate.

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

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

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

- You can use the following CI commands to check the ADSL line statistics.
  CI> wan adsl perfdata
  CI> wan adsl status
  CI> wan adsl linedata far
  CI> wan adsl linedata near
- You can also do it in Web Configurator, Advanced Setup, **Maintenance -> Diagnostic -> DSL Line -> DSL Status:**



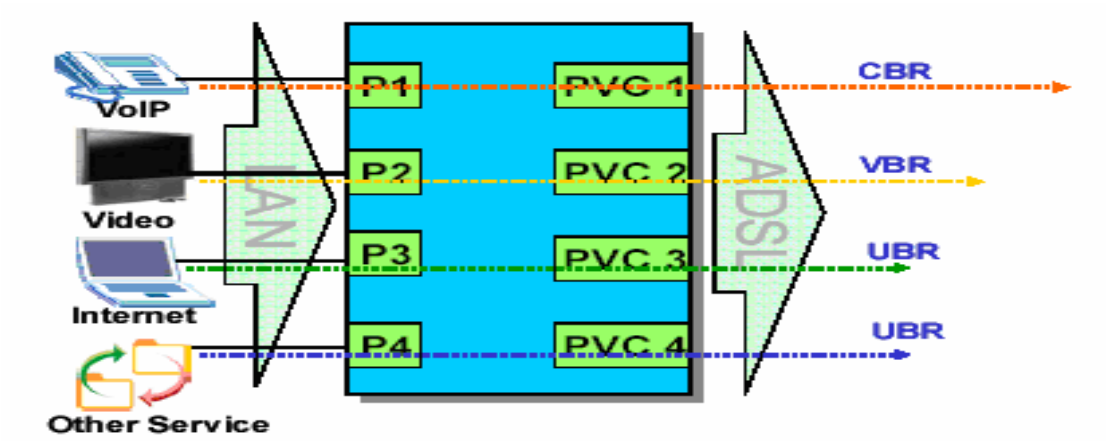

### 8. What are the signaling pins of the ADSL connector?

The signaling pins on the P-661H-D's ADSL connector are pin 3 and pin 4. The middle two pins for a RJ11 cable.

### 9. What is triple play?

More and more Telco/ISPs are providing three kinds of services (VoIP, Video and Internet) over one existing ADSL connection.

- The different services (such as video, VoIP and Internet access) require different Qulity of Service.
- The high priority is Voice (VoIP) data.
- The Medium priority is Video (IPTV) data.
- The low priority is internet access such as ftp etc …




Triple Play is a port-based policy to forward packets from different LAN port to different PVCs, thus you can configure each PVC separately to assign different QoS to different application.

# Firewall FAQ

## 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 P-661H-D secure?

The P-661H-D 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 P-661H-D 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 headers 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 P-661H-D?**

1. The P-661H-D'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 P-661H-D'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 P-661H-D'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 P-661H-D'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 P-661H-D'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. What are the default ACL firewall rules in P-661H-D?

There are two default ACLs pre-configured in the P-661H-D, one allows all connections from LAN to WAN and the other blocks all connections from WAN to LAN except of the DHCP packets.

## Configuration

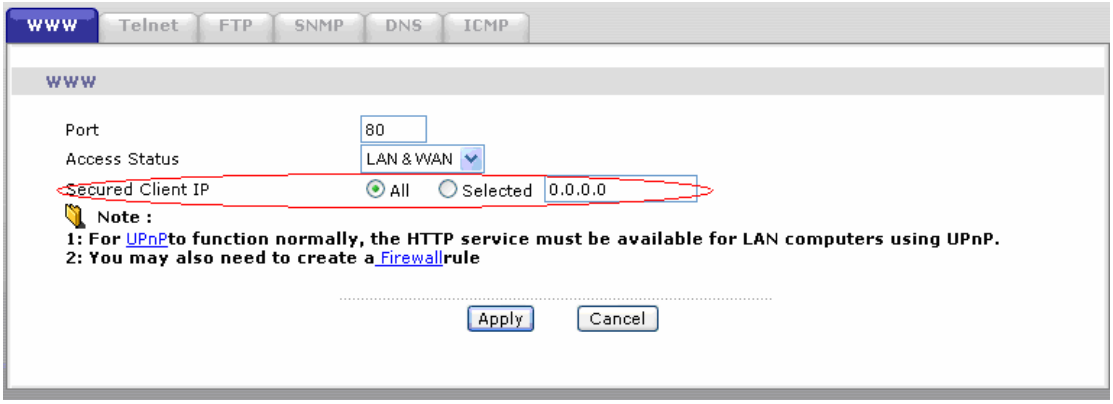
### 1. How do I configure the firewall?

You can use the Web Configurator to configure the firewall for P-661H-D. By factory default, if you connect your PC to the LAN Interface of P-661H-D, you can access Web Configurator via ‘http://192.168.1.1’.
**Note: Don’t forget to type in the Administrator Password.**

### 2. How do I prevent others from configuring my firewall?

There are several ways to protect others from touching the settings of your firewall.

1. Change the default Administrator password since it is required when setting up the firewall.
2. Limit who can access to your P-661H-D's Web Configurator or CLI. You can enter the IP address of the secured LAN host in Web Configurator, Advanced Setup, **Advanced -> Remote MGNT -> [Service] ->Secured Client IP** to allow special access to your P-661H-D:




The default value in this field is 0.0.0.0, which means you do not care which host is trying to telnet your P-661H-D or access.the Web Configurator of

### 3. Why can't I configure my P-661H-D using Web Configurator/Telnet over WAN?

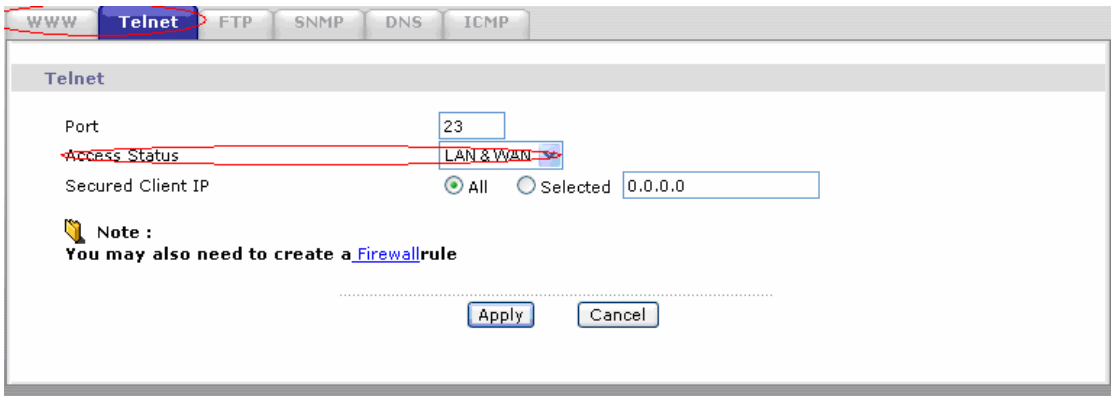
There are four reasons that WWW/Telnet from WAN is blocked.

(1) When the firewall is turned on, all connections from WAN to LAN are blocked by the default ACL rule. To enable Telnet from WAN, you must turn the firewall off, or create a firewall rule to allow WWW/Telnet connection from WAN. The WAN-to-LAN ACL summary will look like as shown below.

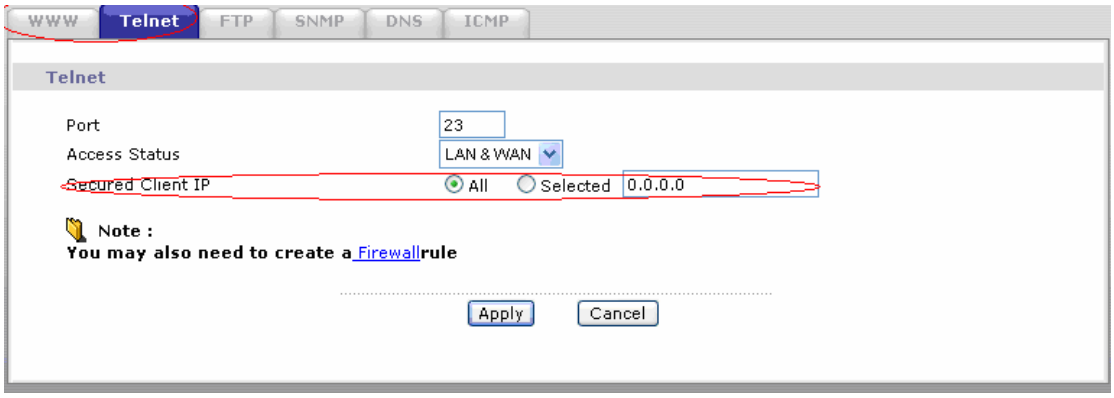
**WWW (For accessing Web Configurator):**
Source IP= Remote trusted host
Destination IP= router' WAN IP
Service= TCP/80
Action=Forward

**TELNET (For accessing Command Line Interface):**
Source IP= Telnet Client host
Destination IP= router' WAN IP
Service= TCP/23
Action=Forward

(2)You have disabled WWW/Telnet service in Web Configurator, Advanced setup, **Advanced -> Remote MGNT:**




(3) WWW/Telnet service is enabled but your host IP is not the secured host entered in Web Configurator, Advanced setup, **Advanced -> Remote MGNT:**




(4)A filter set which blocks WWW/Telnet from WAN is applied to WAN node. You can check by command:
**wan node index [index #]**
**wan node display**

## 4. Why can't I upload the firmware and configuration file using FTP over WAN?

(1) When the firewall is turned on, all connections from WAN to LAN are blocked by the default ACL rule. To enable FTP from WAN, you must turn the firewall off or create a firewall rule to allow FTP connection from WAN. The WAN-to-LAN ACL summary will look like as shown below.

Source IP= FTP host
Destination IP= P-661H-D's WAN IP
Service= FTP TCP/21, TCP/20
Action=Forward

(2) You have disabled FTP service in Web Configurator, Advanced setup, **Advanced -> Remote MGNT.**

(3) FTP service is enabled but your host IP is not the secured host entered in Web Configurator, Advanced setup, **Advanced -> Remote MGNT.**

(4) A filter set which blocks FTP from WAN is applied to WAN node. You can check by command:
**wan node index [index #]**
**wan node display**

## Log and Alert

### 1. When does the P-661H-D generate the firewall log?

The P-661H-D generates the firewall log immediately when the packet matches a firewall rule. The log for Default Firewall Policy (LAN to WAN, WAN to LAN, WAN to WAN) is generated automatically with factory default setting, but you can change it in Web Configurator.

### 2. What does the log show to us?

The log supports up to 128 entries. There are 5 columns for each entry. Please see the example shown below:

| # | Time | Message | Source | Destination | Notes |
|---|---|---|---|---|---|
| 1 | 12/13/2005 15:35:21 | Firewall default policy: TCP (L to W) | 192.168.1.33:3466 | 207.69.188.186:5000 | ACCESS PERMITTED |

### 3. How do I view the firewall log?

All logs generated in P-661H-D, including firewall logs, IPSec logs, system logs are migrated to centralized logs. So you can view firewall logs in Centralized logs: Web Configurator, Advanced setup, **Maintenance -> Logs ->View Log.**

The log keeps 128 entries, the new entries will overwrite the old entries when the log has over 128 entries.

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 Setup, **Maintenance -> 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

- Web Configurator: Advanced setup, **Maintenance -> Logs ->View Log.**
- 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 Web configuration: Advanced Setup, **Maintenance -> Logs -> Log Settings**.

**4. When does the P-661H-D generate the firewall alert?**

The P-661H-D 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, Advanced Setup, **Maintenance -> Logs -> Log Settings**. You can also specify how frequently you want to receive the alert in it.

**5. What is the difference between the log and alert?**

A log entry is just added to the log inside the P-661H-D 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.

# VPN FAQ

## General FAQ

### 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 P-661H-D 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, on Prestige, if "DNS" or "E-mail" type is choosen, you can still use a random string as the content, such as "this_is_Prestige". It's not neccessary to follow the format exactly.

By default, the device 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 ajust the settings to pass phase 1 ID checking.

**15. When should I use FQDN?**

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

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.

**Advanced FAQ**

**1. How do I configure VPN?**

You can configure VPN via Web Configurator, Advanced Setup, **Security -> VPN -> Summary.**

**2. What kind of VPN protocols are supported on P-661H-D?**

All P-661H-D series support IPSec VPN, in other words, we can build IPSec VPN on P-661H-D.

And also note that P-661H-D is of VPN (IPSec, PPTP) passthrough supported NAT.

**3. What types of encryption does P-661H-D VPN support?**

P-661H-D supports DES/3DES/AES encryption.

**4. What types of authentication does P-661H-D VPN support?**

VPN vendors support a number of different authentication methods. P-661H-D 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.

**5. I am planning my P-661H-D VPN configuration. What do I need to know?**

You can find the VPN options in Web Configurator, Advanced Setup, **Security -> VPN.**
For configuring a 'box-to-box VPN', there are some tips:

(1) If there is a NAT router running in the front of P-661H-D, please make sure the NAT router supports IPSec passthrough.

(2) In NAT case, only IPSec tunneling mode is supported. Here's a brief summary for IPSec and NAT:

| NAT Condition | Supported IPSec Protocol |
|---|---|
| VPN Gateway embedded NAT | **AH Tunnel mode,**<br>**ESP Tunnel mode** |

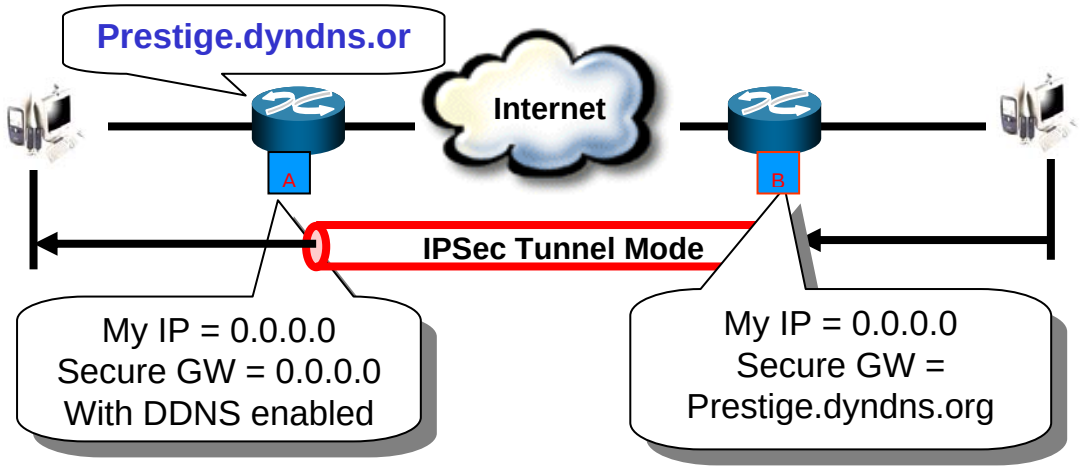
| | |
|---|---|
| VPN Gateway behind NAT | **ESP Tunnel mode** |
| NAT in Transport mode | **None** |

(3) **Source IP/Destination IP**-- Please do not number the LANs (local and remote) using the same range of private IP addresses. This will make VPN destination addresses and the local LAN addresses are indistinguishable, and VPN will not work.
(4) **Secure Gateway IP Address** --It is usually a static IP so that we can pre-configure it in P-661H-D for making VPN connections. If it is a dynamic IP given by ISP, you still can configure this IP address after the remote P-661H-D is on-line and its WAN IP is available from ISP. Or you can use DDNS as below.

**6. Does P-661H-D support dynamic secure gateway IP?**

Yes. If the remote VPN gateway uses dynamic IP, we enter **0.0.0.0** as the **Secure Gateway IP Address** in P-661H-D. In this case, the VPN connection can only be initiated from dynamic side to fixed side in order to update its dynamic IP to the fixed side.
If both gateways use dynamic IP addresses, we can use DDNS on one side. For example:

- Both sides are dynamic IP address
  --- Router A: DDNS enabled
  --- Router B: Secure GW = DNS name




With DDNS support, through the Router A's WAN IP changes time to time, the DNS name of router A is still valid. Router B could establish VPN tunnels with router A by specifying ASecure GW as Router A's DNS name, even if router B itself is dynamic IP address too. Note: In the example, the VPN connection can only be initiated from Router B.

**7. What VPN gateway has been tested with P-661H-D successfully?**

We have tested P-661H-D successfully with the following third party VPN gateway:

- 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
- Avaya VPN
- Netopia VPN
- III VPN

**8. What VPN software has been tested with P-661H-D successfully?**

We have tested P-661H-D successfully with the following third party VPN software.

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

**9. What is the difference between the 'My IP Address' and 'Secure Gateway IP Address' in VPN Setup Web Page?**

**'My IP Adderss**' is the Internet IP address of the local P-661H-D. The **'Secure Gateway IP Address'** is the Internet IP address of the remote IPSec gateway.

**10. Is the host behind NAT allowed to use IPSec?**

| NAT Condition | Supported IPSec Protocol |
|---|---|
| VPN Gateway embedded NAT | AH tunnel mode, ESP tunnel mode |
| VPN client/gateway behind | ESP tunnel mode |

| | |
|---|---|
| NAT* | |
| NAT in Transport mode | None |

* The NAT router must support IPSec pass through. For example, for P-661H-D SUA/NAT routers, the default port and the client IP have to be specified in Web Configurator, **Network -> NAT ->SUA Server Setup.**

**11. How do I configure P-661H-D 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 P-661H-D, the edit of the table is necessary only if the connection is a non-secure connection. For secure connections, none SUA server settings are required since private IP is reachable in the VPN case.

**12. I am planning my P-661H-D behind a NAT router. What do I need to know?**

Suppose: host----P-661H-D----NAT Router----Internet----Secure host
Some tips for the configuration:
(1) The NAT router must support to pass through IPSec protocol. Only ESP tunnel mode is possible to work in NAT case. Default port (UDP Port 500) and the P-661H-D's WAN IP must be configured in NAT Router's SUA/NAT Server Table.
(2) On the Secure host side, WAN IP of the NAT router is the tunneling endpoint for this case, not the WAN IP of P-661H-D.
For example:
On P-661H-D: My IP Address= P-661H-D's WAN IP
Secure Gateway IP Address= Secure host's IP
On Secure host: My IP Address= Secure host's IP
Secure Gateway IP Address= NAT Router's WAN IP

**13. 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.

### 14. Single, Range, Subnet, which types of IP address do P-661H-D support in VPN/IPSec?

P-661H-D supports all of the types. In other words, you can specify a single PC, a range of PCs or even a network of PCs to utilize the VPN/IPSec service.

### 15. Can P-661H-D support VPN passthrough?

Yes, P-661H-D can support VPN (IPSec, PPTP) passthrough. P-661H-D series don't only support IPSec/VPN gateway, it can also be a NAT router supporting VPN (IPSec, PPTP) passthrough.
If the VPN connection is initiated from the security gateway behind P-661H-D, no configuration is necessary for NAT/ Firewall.
If the VPN connection is initiated from the security gateway outside of P-661H-D, NAT port forwarding and Firewall forwarding are necessary.
To configure NAT port forwarding, please go to Web Configurator, **Network -> NAT -> Port Forwarding,** put the secure gateway's IP address in default server.
To configure Firewall forwarding, please go to Web Configurator, **Security -> Firewall -> Rules**, select Packet Direction **WAN to LAN**, and create a firewall rule that forwards IKE(UDP:500).

### 16. Can P-661H-D behave as a NAT router supporting IPSec passthrough and an IPSec gateway simultaneously?

No, P-661H-D can't support them simultaneously. You need to choose either one. If P-661H-D is to support IPSec passthrough, you have to disable the VPN function on P-661H-D. To disable it, you can either deactivate each VPN rule or issue a CI command, "**ipsec switch off**" from **CLI**.

# Application Notes

## General Application Notes

### 1. Internet Access Using P-661H-D under Bridge mode

- Setup your workstation
- Setup your P-661H-D under bridge mode

If the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use P-661H-D which works as an ADSL bridge modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

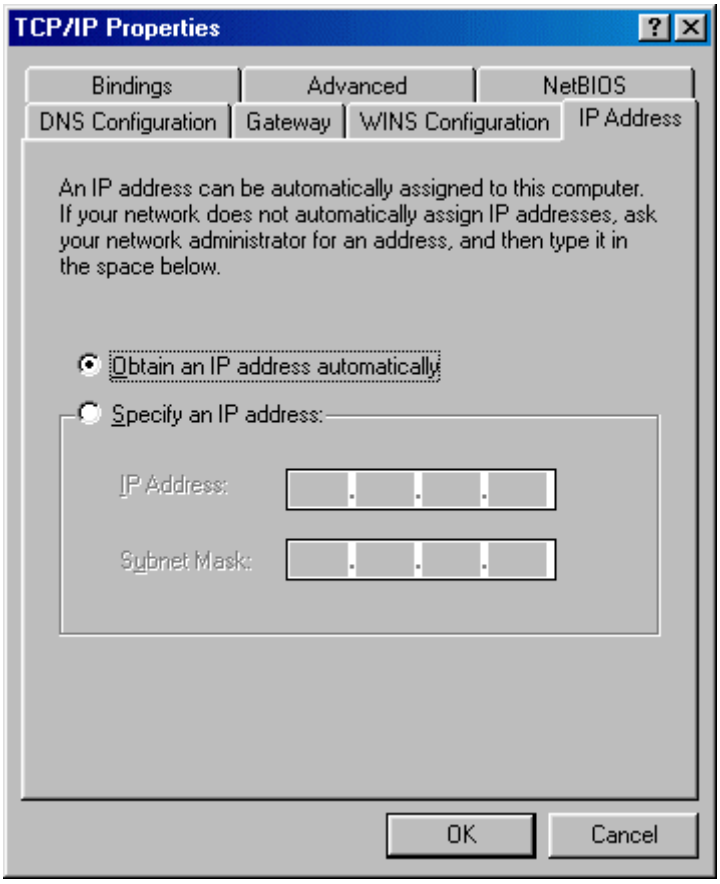
### Set up your workstation

#### (1) Ethernet connection

To connect your computer to the P-661H-D's LAN port, the computer must have an Ethernet adapter card installed. For connecting a single computer to the P-661H-D, we use a Ethernet cable.

#### (2) TCP/IP configuration

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

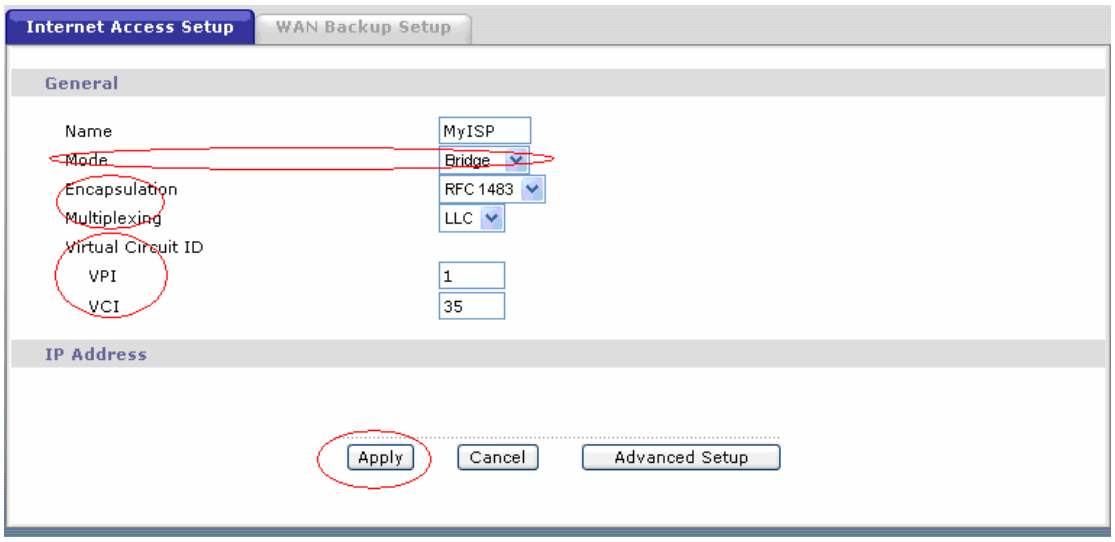



## Setup your P-661H-D under bridge mode

The following procedure shows you how to configure your P-661H-D as bridge mode. We will use Web Configurator to guide you through the related menu.

(1) Configure P-661H-D as bridge mode and configure Internet setup parameters in Web Configurator, Advanced Setup, **Network -> WAN ->**

**Internet Connection.**




Key Settings:

| Option | Description |
|---|---|
| Encapsulation | Select the correct Encapsulation type that your ISP supports. For example, RFC 1483. |
| Multiplexing | Select the correct Multiplexing type that your ISP supports. For example, LLC. |
| VPI & VCI number | Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP. |

(2) Turn off DHCP Server and configure a LAN IP for the P-661H-D in Web Configurator, Advanced Setup, **Network -> LAN**. We use 192.168.1.1 as the LAN IP for P-661H-D in this case:

Step 1: Disactive DHCP Server and apply it:

Step 2: Assign an IP to the LAN Interface of P-661H-D, e.g.: 192.168.1.1:

**2. Internet Access Using P-661H-D under Routing mode**

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to install an Internet sharing device, like a router. In this case, we use the P-661H-D which works as a general Router plus an ADSL Modem.

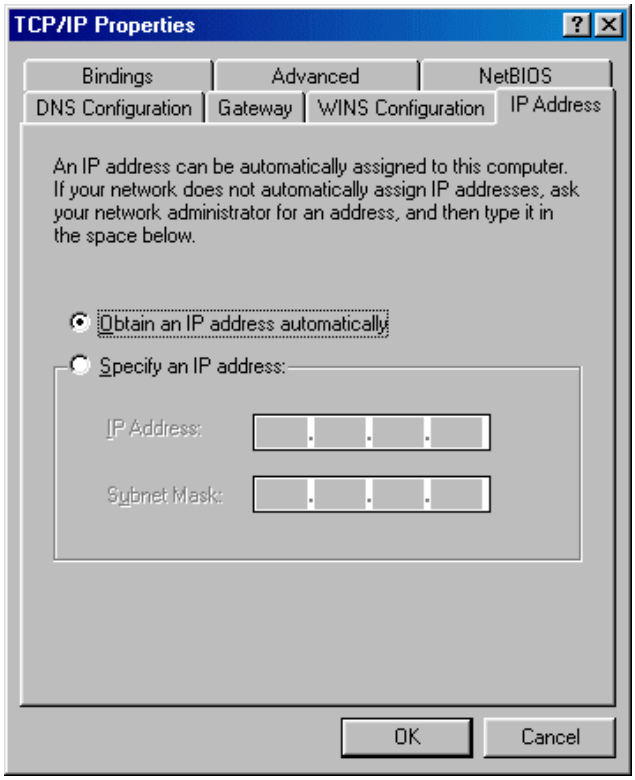
**Set up your workstation**

**(1) Ethernet connection**

Connect the LAN ports of all computers to the LAN Interface of P-661H-D using Ethernet cable.

**(2) TCP/IP configuration**

Since the P-661H-D is set to DHCP server as default, so you need only to configure the workstations as the DHCP clients in the networking settings. In this case, the IP address of the computer is assigned by the P-661H-D. The P-661H-D can also provide the DNS to the clients via DHCP if it is available. For this setup in Windows, we check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup. Please see the example shown below.




## Set up your P-661H-D under routing mode

The following procedure shows you how to configure your P-661H-D as Routing mode for routing traffic. We will use Web Configurator to guide you through the related menu.

(1) Configure P-661H-D as routing mode and configure Internet setup parameters in Web Configurator, Advanced Setup, **Network -> WAN -> Internet Connection.**

Key Settings:

| Option | Description |
|---|---|
| Encapsulation | Select the correct Encapsulation type that your ISP supports. For example, RFC 1483. |
| Multiplexing | Select the correct Multiplexing type that your ISP supports. For example, LLC. |
| VPI & VCI number | Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP. |
| IP Address Assignment | Set to **Dynamic** if the ISP provides the IP for the P-661H-D dynamically. Otherwise, set to **Static** and enter the IP in the **IP Address** field. |

(2) Configure a LAN IP for the P-661H-D and the DHCP settings in Web Configurator, Advanced Setup, **Network -> LAN.**

### 3. Setup the P-661H-D as a DHCP Relay

- **What is DHCP Relay?**

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P-661H-D supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the LAN clients. When it is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 1.

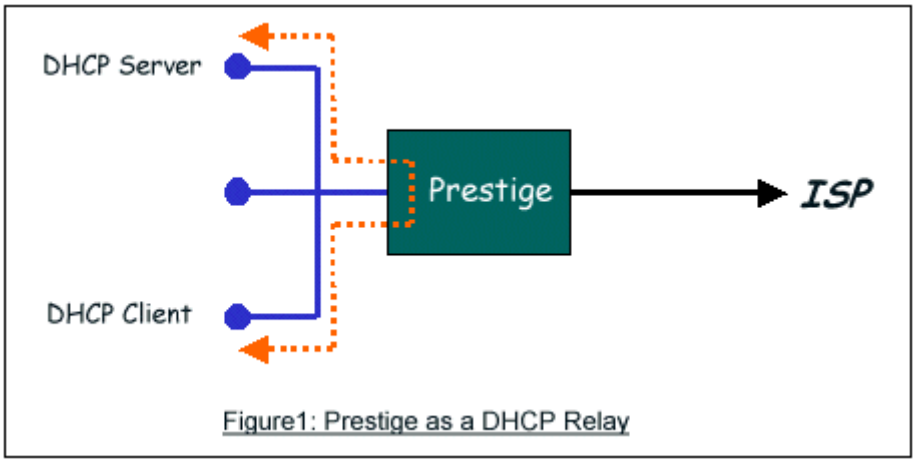


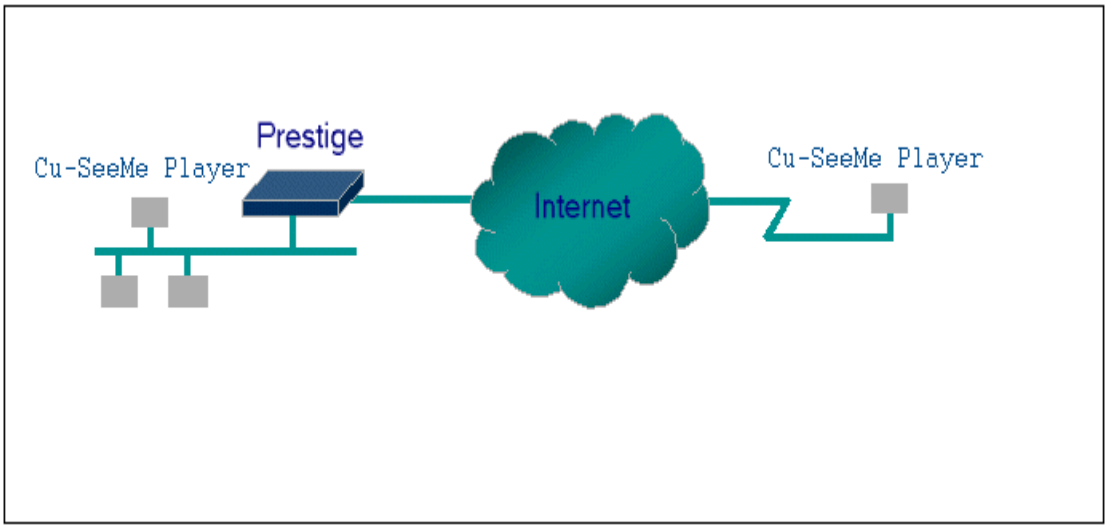
Figure1: Prestige as a DHCP Relay

- **Setup the P-661H-D as a DHCP Relay**

We could set the P-661H-D as a DHCP Relay by the following command in **CLI**:
**Ip dhcp enif0 mode relay**
**Ip dhcp enif0 relay server [Server IP Address]**

## 4. SUA Notes

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




**Introduction**

Generally, SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. However, some applications such as Cu-SeeMe, and ICQ will need to connect to the local user behind the P-661H-D. In such case, a SUA server must be configured to forward the incoming packets to the true destination behind SUA. After the required server are configured in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding,** the internal server or client applications can be accessed by using the P-661H-D's ***WAN IP* Address**.

**SUA Supporting Table**

The following are the required Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** for the various applications running SUA mode.

ZyXEL SUA Supporting Table[1]

| Application | Required Settings in **Port Forwarding** Port/IP | |
|---|---|---|
| | Outgoing Connection | Incoming Connection |
| HTTP | None | 80/client IP |
| FTP | None | 21/client IP |
| TELNET | None | 23/client IP (and active Telnet service from WAN) |
| POP3 | None | 110/client IP |
| SMTP | None | 25/client IP |

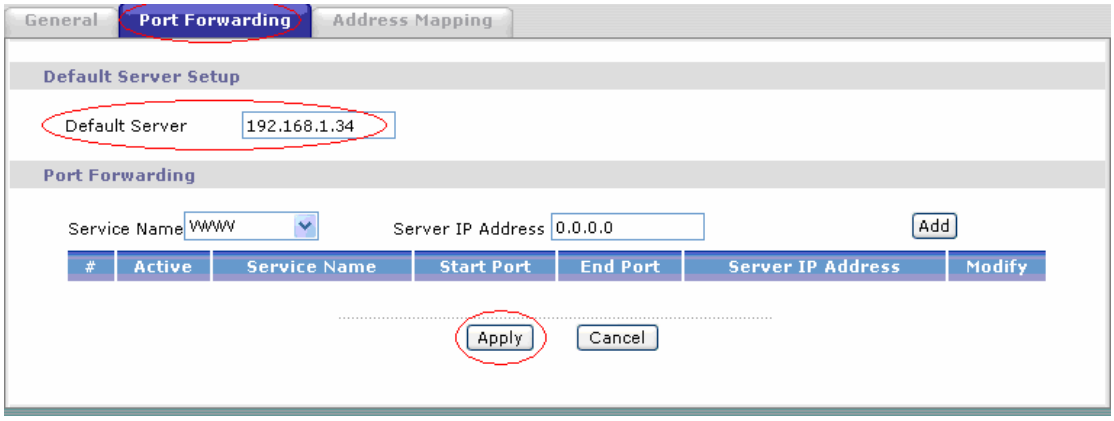
| | | |
|---|---|---|
| mIRC | None for Chat.<br>For DCC, please set Default/Client IP | . |
| Windows PPTP | None | 1723/client IP |
| ICQ 99a | None for Chat.<br>For DCC, please set:<br>ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting. | Default/client 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 &<br>24032/client IP | Default/client IP |
| White Pine 4.0 Cu-SeeMe | 7648/client IP &<br>24032/client IP | Default/client IP |
| Microsoft NetMeeting 2.1 & 3.01[3] | None | 1720/client IP<br>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<br>5632/client IP<br>22/client IP |
| IPsec (ESP tunneling mode) | None (one client only) | Default/Client |
| Microsoft Messenger Service 3.0 | 6901/client IP | 6901/client IP |
| Microsoft Messenger Service 4.6/ 4.7/ 5.0/…<br>(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<br>5800/client IP<br>5900/client IP |
| AIM (AOL Instant Messenger) | None for Chat and IM | None for Chat and IM |
| e-Donkey | None | 4661 - 4662/client IP |
| POLYCOM Video Conferencing | None | Default/client IP |
| iVISTA 4.1 | None | 80/server IP |
| Microsoft Xbox Live[7] | None | N/A |

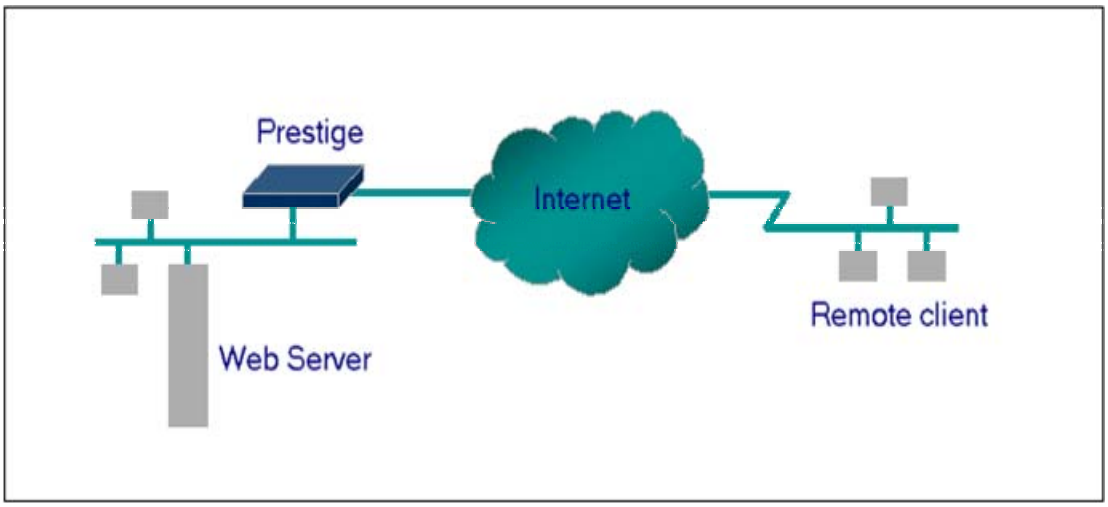
[1] Since SUA enables your LAN to appear as a single computer to the Internet, it is not possible to configure similar servers on the same LAN behind SUA.
[2] Because White Pine Cu-SeeMe uses dedicate ports (port 7648 & port 24032) to transmit and receive data, therefore only one local Cu-SeeMe is allowed within the same LAN.
[3] In SUA mode, only one local NetMeeting user is allowed because the outsiders can not distinguish between local users using the same internet IP.
[4] Certain Quake servers do not allow multiple users to login using the same unique IP, so only one Quake user will be allowed in this case. Moreover, when a Quake server is configured behind SUA, P-661H-D will not be able to provide information of that server on the internet.
[5] Quake II has the same limitations as that of Quake I.
[6] P-661H-D supports 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 P-661H-D is an alternative solution to pass through MSN Messenger video/ voice traffic. For more detail, please refer to UPnP application note.
[7] P-661H-D support Microsoft Xbox Live with factory default configuration.

**Configurations**

For example, if the workstation operating Cu-SeeMe has an IP of 192.168.1.34, then the default SUA server must be set to 192.168.1.34. The peer Cu-SeeMe user can reach this workstation by using P-661H-D's ***WAN IP*** address which can be obtained from Web Configurator, **Status -> WAN Information**.




## 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 behind the P-661H-D, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time P-661H-D 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 is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

## Configuration

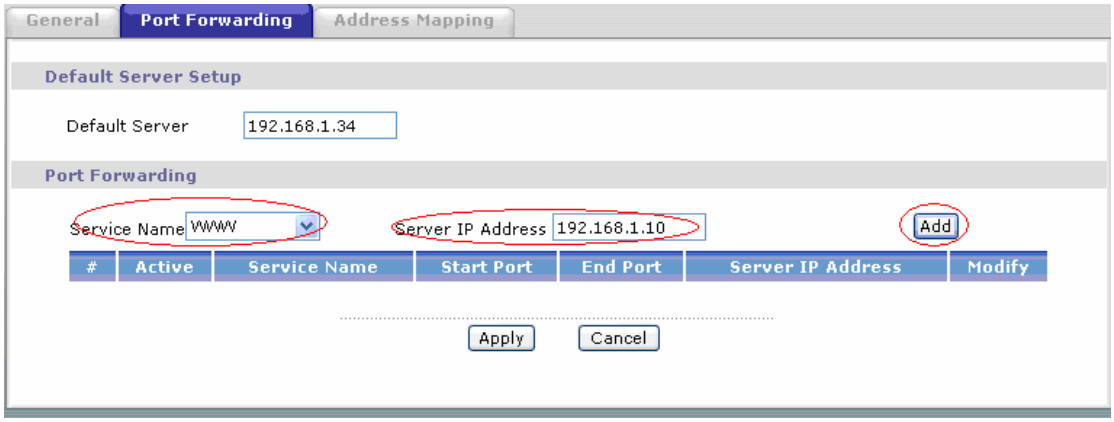
To make a server visible to the outside world, specify the port number of the service and the inside address of the server in Web Configurator, Advanced

Setup, **Network -> NAT -> Port Forwarding.** The outside users can access the local server using the P-661H-D's ***WAN IP*** address which can be obtained from Web Configurator, **Status -> WAN Information**.

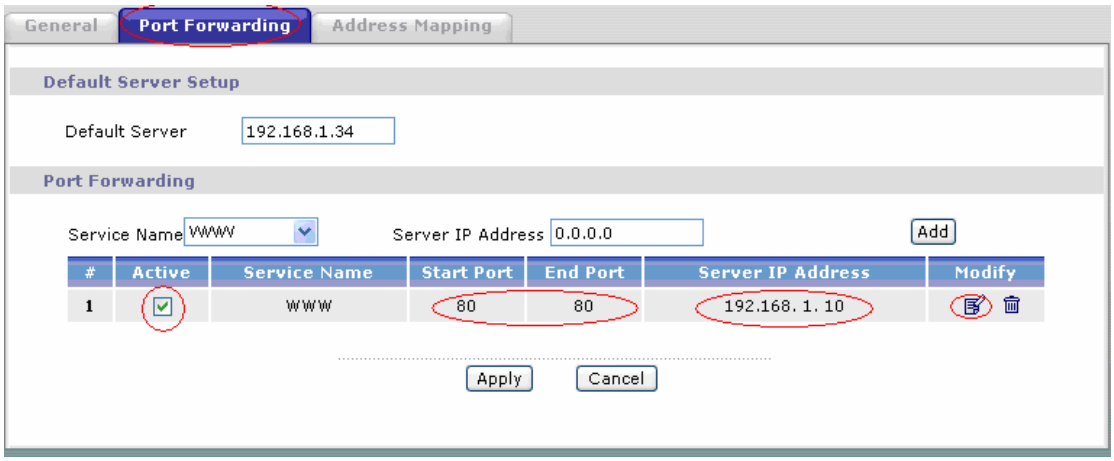
For example:

**Configuring an internal Web server for outside access** (suppose the Server IP Address is 192.168.1.10 ) :

(1) Fill in the service name and server IP Address, press button 'Add'




(2) If add successfully, the Web Configurator will display message 'Configuration updated successfully' at the bottom. You can see the port forwarding rule on the same page, the default port for Web Server is 80:




(3) If you want to change the port for Web Server, you could press button 'Modify' on corresponding rule, then modify and apply it.

**Default port numbers for some services**

| Service | Port Number |
|---|---|

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

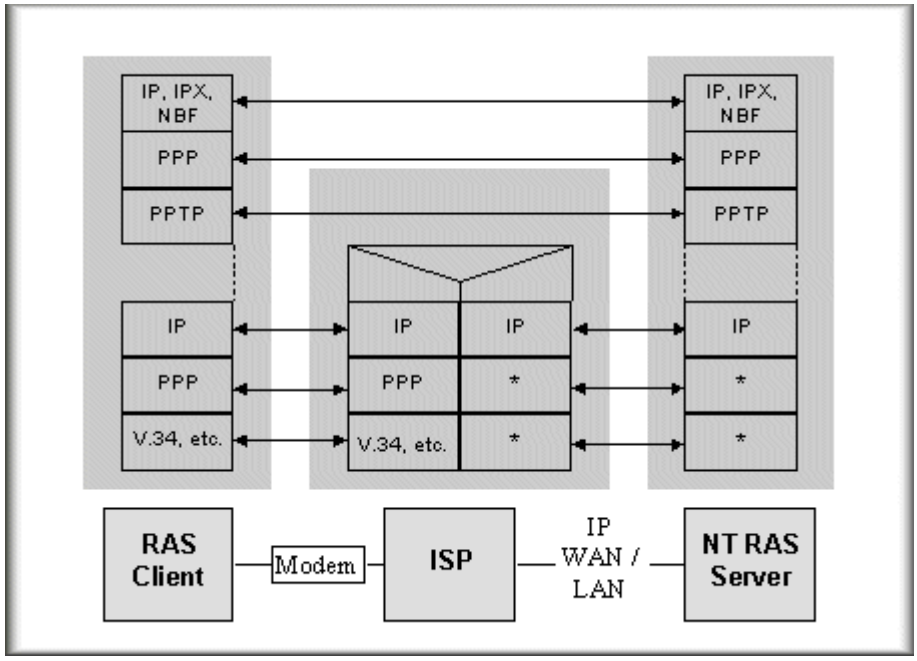
**Configure a PPTP server behind SUA**

Introduction

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

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

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



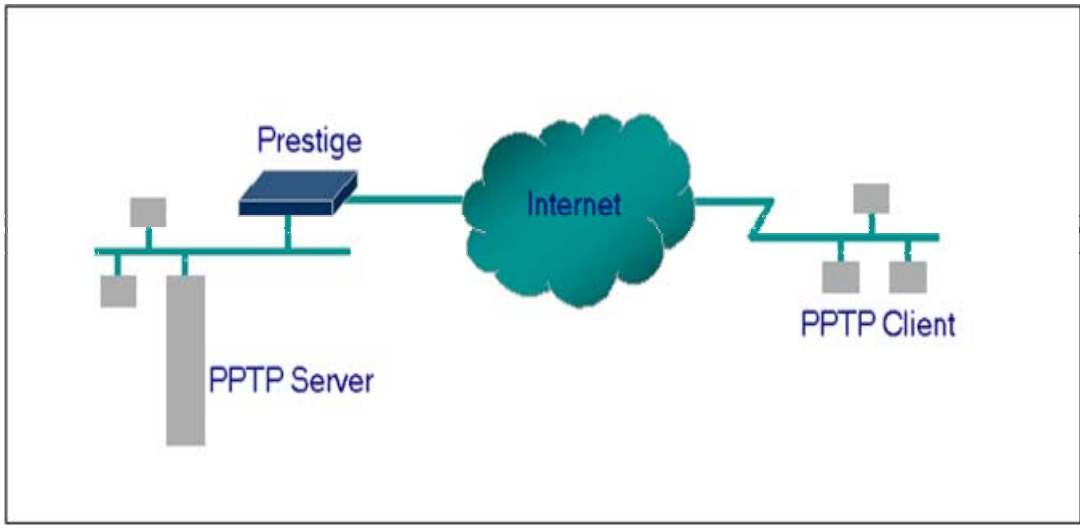

Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

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

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

Configuration

This application note explains how to establish a PPTP connection with a remote private network in the P-661H-D 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 Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** on P-661H-D to forward to the appropriate private IP address of Windows NT server.




Example

The following example shows how to dial to an ISP via the P-661H-D and then establish a tunnel to a private network. There will be three items that you need to set up for PPTP application, these are PPTP server (WinNT), PPTP client (Win9x) and the P-661H-D.

(1) PPTP server setup (WinNT)

- Add the VPN service from Control Panel ->Network
- Add an user account for PPTP logged on user
- Enable RAS port
- Select the network protocols from RAS such as IPX, TCP/IP NetBEUI
- Set the Internet gateway to P-661H-D

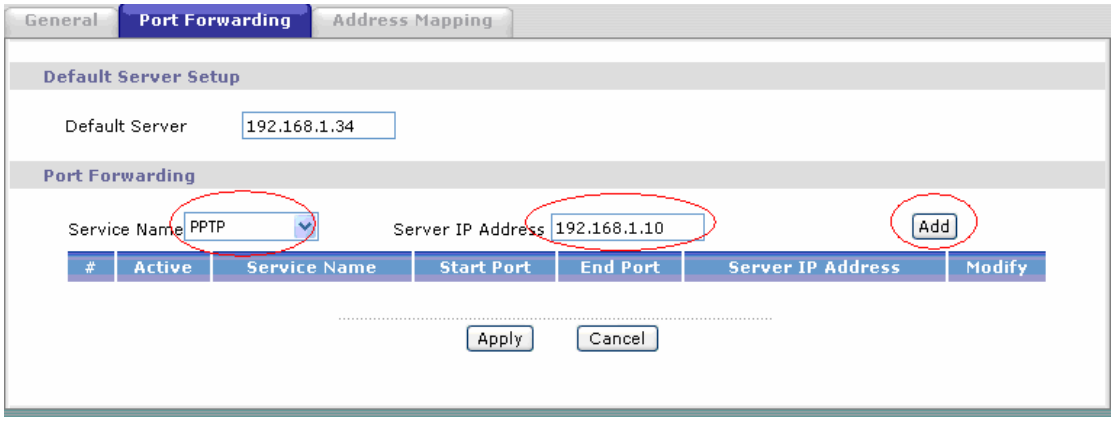
(2) PPTP client setup (Win9x)

- Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the P-661H-D's Internet IP address for logging to NT RAS server.
- Set the Internet gateway to the router that is connecting to ISP

(3) P-661H-D setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect P-661H-D router to your ISP first.
- Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown below:

Select service name as ‘PPTP’, fill in the Server IP Address, then press button ‘Add’.



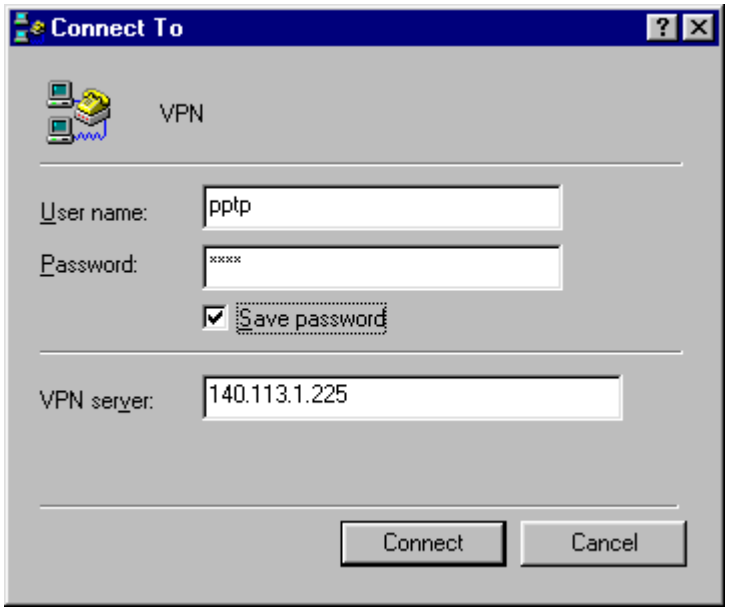

When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the Internet. If the Internet connection between two LANs is achievable, you can place a VPN call from the remote Win9x client.

For example: C:\ping 203.66.113.2

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

Before making a VPN connection from the Win9x client to the NT server, you need to know the exact Internet IP address that the ISP assigns to P-661H-D 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 S Web Configurator, **Status -> WAN Information**. 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.




## 5. Using Full Feature NAT

**When P-661H-D is in Routing mode, you can select NAT Option as Full Feature in** Network -> Remote Node -> Edit:


Key Settings:

| Field | Options | Description |
|---|---|---|
| Network Address Translation | **Full Feature** | When you select this option you can select Address Mapping Set Number 1~8 in the pull-down menu on the right. |
| | **None** | NAT is disabled when you select this option. |
| | **SUA Only** | When you select this option, this remote node will use default SUA Address Mapping Set. You can see it in CLI by command '**ip nat lookup 255**'. It's a read-only sets with two rules: **Many-to-One** and **server** mapping. Select **Full Feature** when you require other mapping types. |

## Configuring NAT

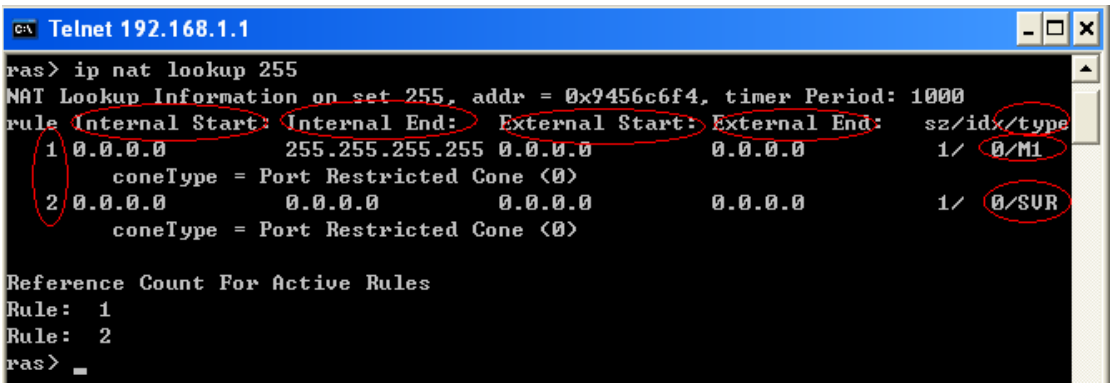
Address Mapping Sets and NAT Server Sets

The P-661H-D has 8 remote nodes and so allows you to configure 8 NAT Address Mapping Sets, You must specify which NAT Address Mapping Set (1~8) to use in the remote node when you select **Full Feature NAT.**

You can edit 10 rules for each Address Mapping Set. You can edit the rules for Address Mapping Sets #1 in Web Configurator. The other Address Mapping Sets #2~8 can only be configured in CLI (Command Line Interface).

The NAT Server Set is a list of LAN side servers mapped to external ports. We can configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding.** To use the NAT server sets you've configured, a **Server** rule must be set up inside the NAT Address Mapping set. Please see NAT Server Sets for further information on how to apply it.

When you select **SUA Only,** the P-661H-D will use a default SUA Address Mapping set for it. It has two rules: **Many-to-One** and **Server**. You can see it in **CLI** by command '**ip nat lookup 255**':




Please note that the fields in this menu are read-only. However, the settings of the rule set 2 can be modified in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding.** The following table explains the fields in this above screen:

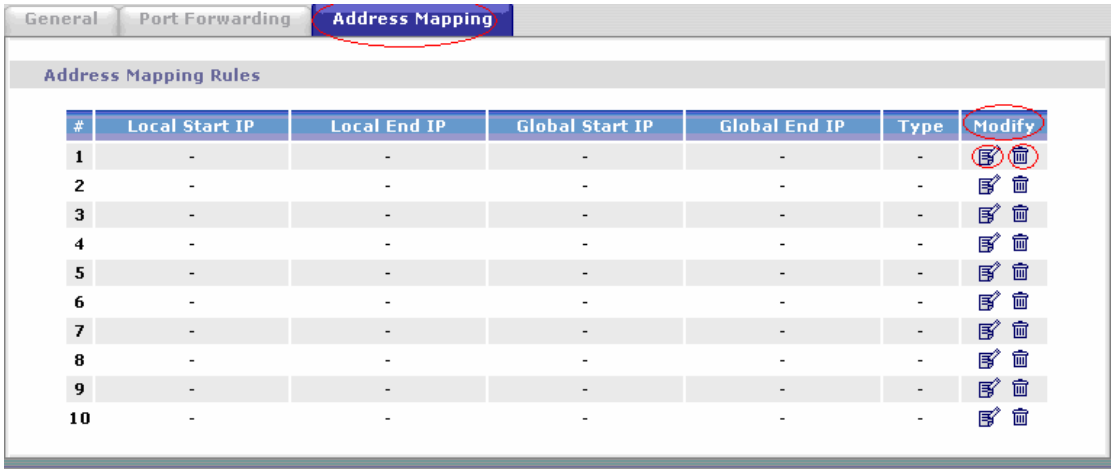
| Field | Description | Option/Example |
|---|---|---|
| set | This is sequence number for Address Mapping Sets | 255 for SUA |
| Internal Start IP | This is the starting local IP address (ILA). | 0.0.0.0 for the Many-to-One type. |
| Local End IP | This is the starting local IP address (ILA). If the 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 | 0.0.0.0 |

| | | |
|---|---|---|
| | IP. | |
| 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 |

Here we'll guide you to configure Address Mapping Sets from **Web Configurator** and **CLI**. (Since in **Web Configurator** we can only edit the rules for Address Mapping Sets #1. The other Address Mapping Sets #2~8 can only be configured in **CLI**)

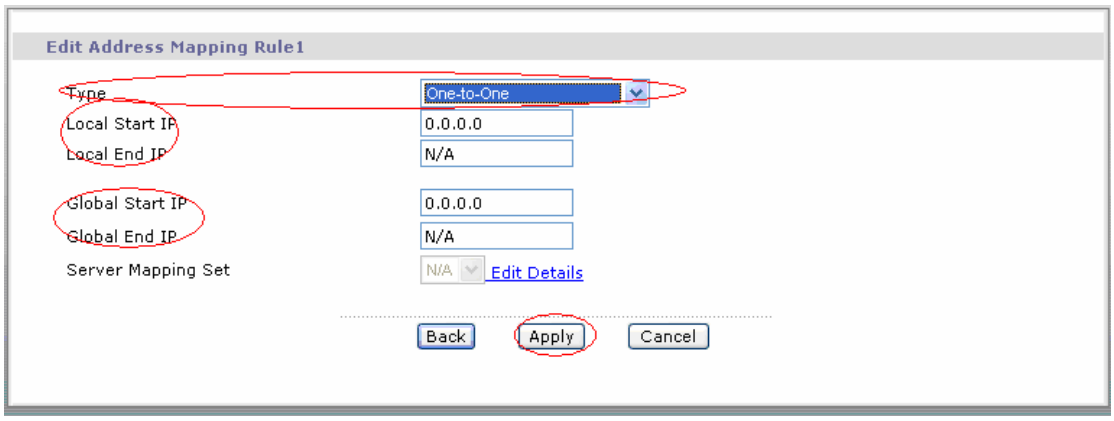
- **Now let's begin with Web Configurator:**

Firstly let's come to Web Configurator, Advanced Setup, **Network -> NAT -> Address Mapping:**




This menu is for Address Mapping Set #1, you can edit 10 Address Mapping Rules for Set #1. You can edit or remove a rule by clicking the two buttons on the rule table.

Click the '**Edit'** Button on the rule #1, then you can enter the window in which you can edit an individual rule and configure the Mapping Type, Local and Global Start/End IPs:




The following table describes the fields in this screen.

| Field | | Description | Option/Example |
|---|---|---|---|
| Type | | You can select one of the five mapping types from the pull-down menu | 1. One-to-One<br>2. Many-to-One<br>3. Many-to-Many Overload<br>4. Many-to-Many No Overload<br>5. Server |
| Local IP | Start | This is the starting local IP address (ILA) | 0.0.0.0 |
| | End | This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for **One-to-One** type. | 255.255.255.255 |
| Global IP | Start | This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**. | 0.0.0.0 |
| | End | This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** types. | 200.1.1.64 |

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

- **Configure Address Mapping Sets in CLI**

**Setp 1:** Telnet to the P-661H-D. (We suppose the LAN IP Address of P-661H-D is 192.168.1.1)
**Step 2:** Select one Address Mapping Set (#1~#8) by command '**ip nat addrmap map [map #] [set name]**' (set name is optional). Suppose we configure set 2 in the example.

**Setp 3:** Set NAT address mapping rule for the Address Mapping Set you just configured (Set 2 in this example) by command '**ip nat addrmap rule [rule#] [insert | edit] [type] [local start IP] [local end IP] [global start IP] [global end IP] [server set #]**'. Suppose we set a Many-to-One rule for set 2 by command '**ip nat addrmap rule 1 edit 1 192.168.1.10 192.168.1.20 172.1.1.1 172.1.1.1**'

**Setp 4:** Save the configuration by command '**ip nat addrmap save**'. You can apply the Address Mapping Set 2 to remote nodes in Web Configurator when you select Full Feature NAT. See the intire process as follows:

```
ras> ip nat addrmap map 2 Test
ras> ip nat addrmap rule 1 edit 1 192.168.1.10 192.168.1.20 172.1.1.1 172.1.1.1
CONFIG NAT Address MAP set:2 rule:1
 ras> ip nat addrmap save
ip nat addrmap: save ok
```

**Set 5:** You can lookup the successfully configured Address Mapping Sets by command '**ip nat addrmap disp**'

```
ras> ip nat addrmap disp
Set Number: 2
Set Name: dis
 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
   1. 192.168.1.10     192.168.1.20     172.1.1.1                         M-1
```

### Key Settings:

| CI Command | Description |
|---|---|
| ip nat addrmap map [map#] [set name] | Select NAT address mapping set and set mapping set name, but set name is optional<br>Example:<br>> ip nat addrmap map 2 Test |
| ip nat addrmap rule [rule#] [insert \| edit] [type] [local start IP] [local end IP] [global start IP] [global end IP] [server set #] | Set NAT address mapping rule. If the "type" is not "inside-server" then the "type" field will still need a dummy value like "0".<br>Type is 0 - 4 = one-to-one, many-to-one, many-to-many-overload, many-to-many-non overload, inside-server<br>Example:<br>> ip nat addrmap rule 1 edit 3 192.168.1.10 192.168.1.20 172.1.1.1 172.1.1.1 |
| ip nat addrmap clear [map#] [rule#] | Clear the selected rule of the set |
| ip nat addrmap freememory | Discard Changes |
| ip nat addrmap disp | Display nat set information |
| ip nat addrmap save | Save settings |
| ip nat server load [set#] | Load the server sets of NAT into buffer |
| ip nat server disp [1] | "disp 1" means to display the NAT server set in buffer, if parameter "1" is omitted, then it will display all the |

| | |
|---|---|
| | server sets |
| ip nat server save | Save the NAT server set buffer into flash |
| ip nat server clear [set#] | Clear the server set [set#], must use “save” command to let it save into flash |
| ip nat server edit [rule#] active | Activate the rule [rule#], rule number is 1 to 24, the number 25-36 is for UPNP application |
| ip nat server edit [rule#] svrport <start port> <end port> | Configure the port range from <start port > to <end port> |
| ip nat server edit [rule#] remotehost <start IP> <end IP> | Configure the IP address range of remote host (Leave it to be default value if you don’t need this command) |
| ip nat server edit [rule#] leasetime <seconds> | Configure the lease time (Leave it to be default value if you don’t want this command) |
| ip nat server edit [rule#] rulename <string> | Configure the name of the rule (Leave it to be default value if you don’t want this command) |
| ip nat server edit [rule#] forwardip <IP address> | Configure the LAN IP address to be forwarded |
| ip nat server edit [rule#] protocol <TCP\|UDP\|ALL> | Configure the protocol to be used TCP , UDP or ALL (it must be capital) |

### 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.

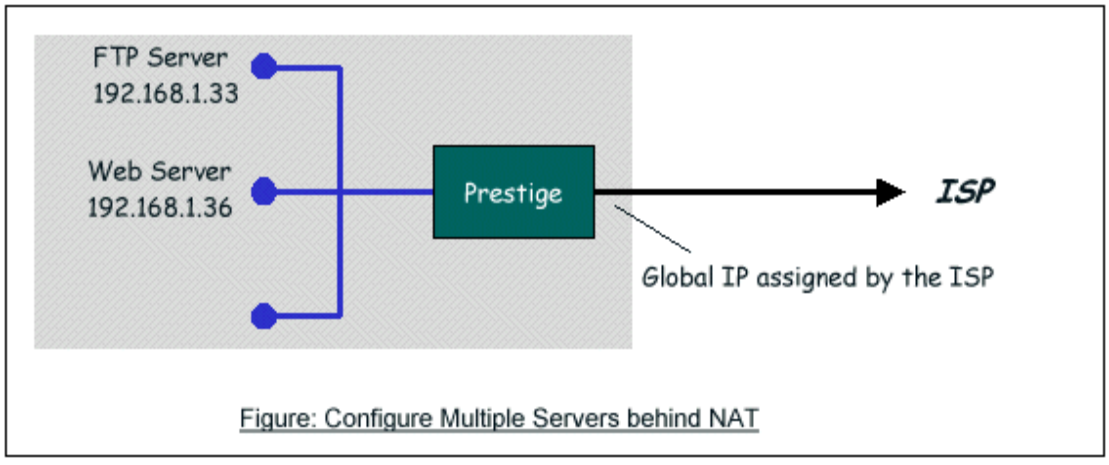


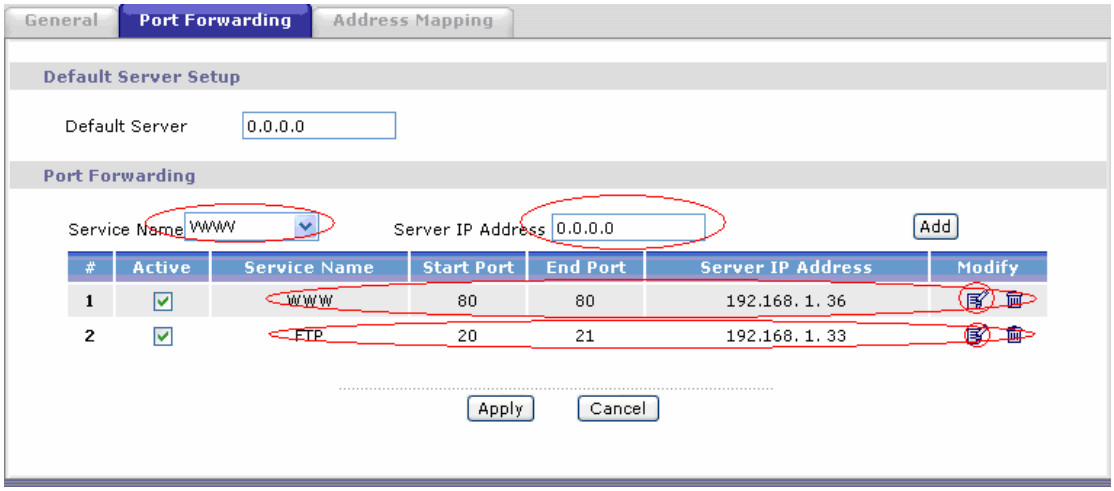

Figure: Configure Multiple Servers behind NAT

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: Login Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding.**

Step 2: Select the service name from the pull-down menu, and fill in the server Address on '**Server IP Address**', then click button '**Add**' to save it.




Step 3: You could click the button 'Edit' on the rule to modify the Service name, Server IP Address, Start/End Port.

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

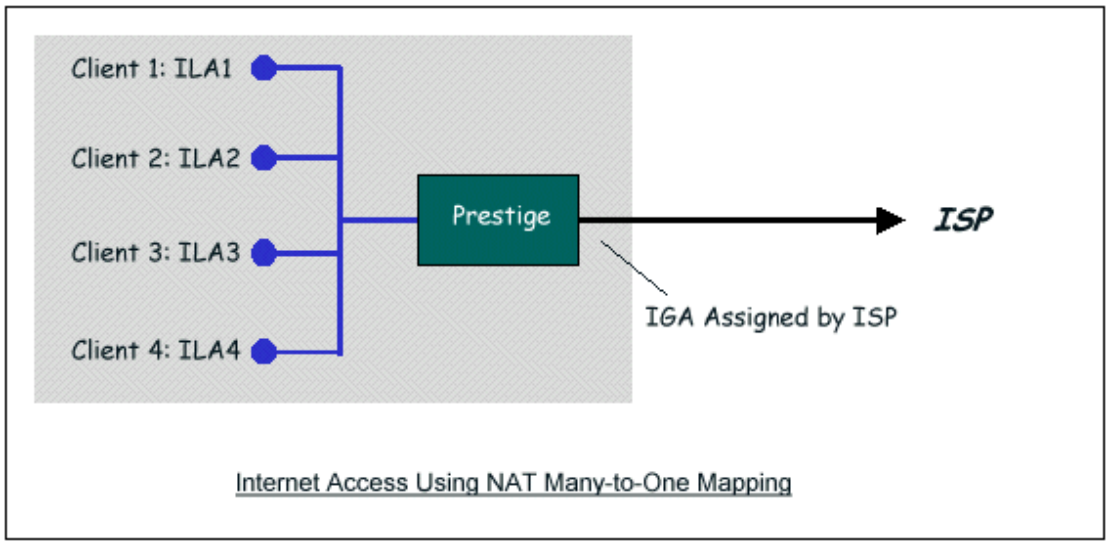
| Service | Port Number |
|---|---|
| FTP | 21 |
| Telnet | 23 |
| SMTP | 25 |
| DNS (Domain Name Server) | 53 |
| www-http (Web) | 80 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

- **Examples**

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

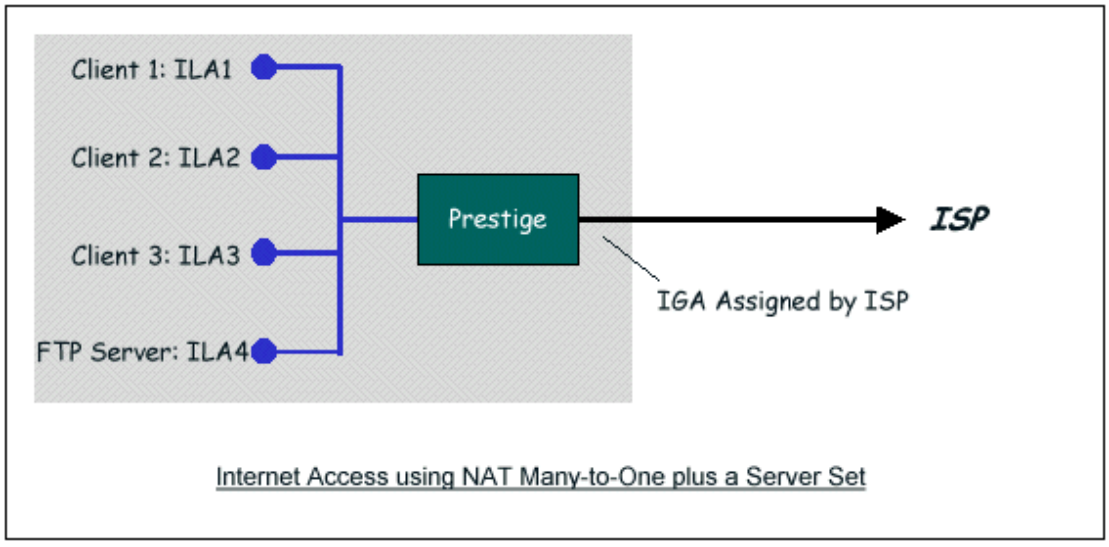
**(1) Internet Access Only**

In our Internet Access example, we only need one rule where all our ILAs map to one IGA assigned by the ISP. You can just use the default **SUA NAT**, or you could select **Full Feature NAT** and select an Address Mapping Set with a **Many-to-One** Rule. See the following figure.




Internet Access Using NAT Many-to-One Mapping

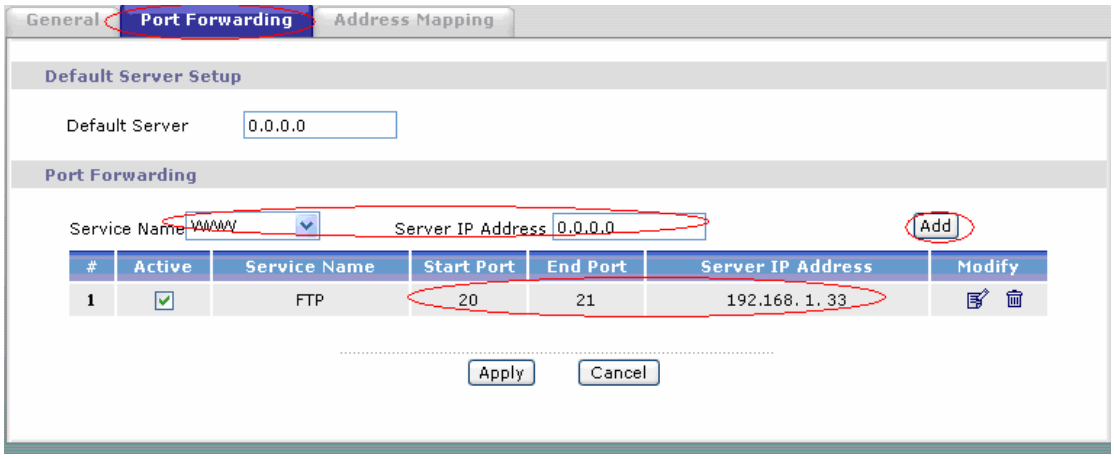
**(2) Internet Access with an Internal Server**



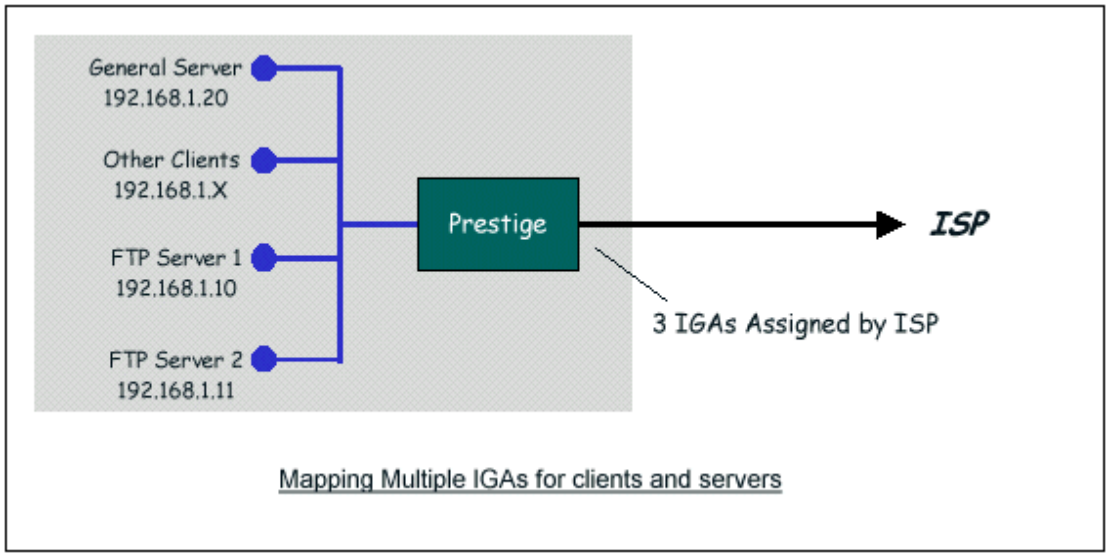

Internet Access using NAT Many-to-One plus a Server Set

In this case, we do exactly as the figure (use the convenient pre-configured SUA Only set) and also go to Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** to specify the Internet Server behind the NAT as

below:



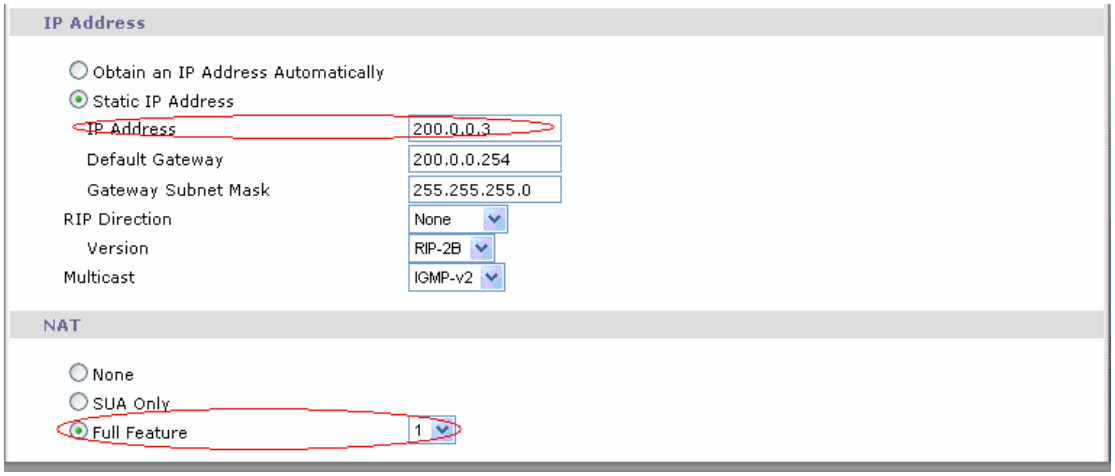

### (3) Using Multiple Global IP addresses for clients and servers (One-to-One, Many-to-One, Server Set mapping types are used)




In this case we have 3 IGAs 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.

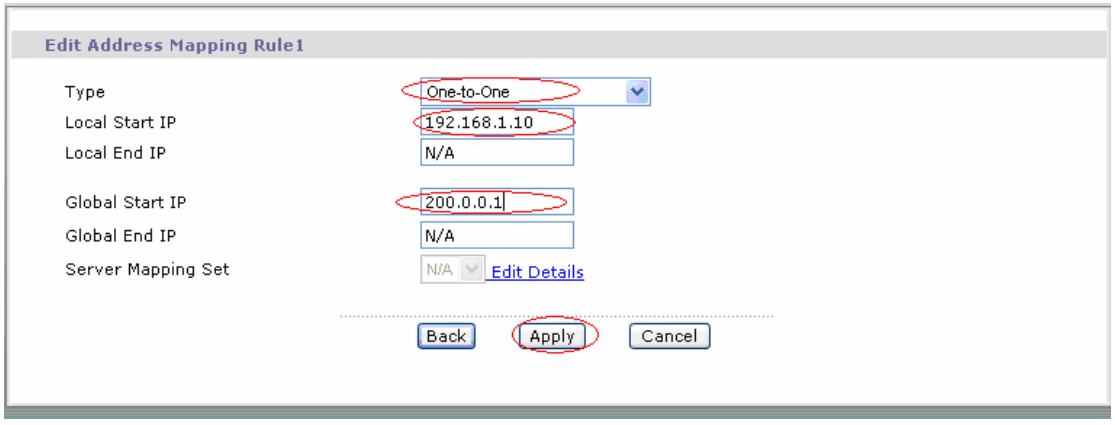
- Rule 1 (One-to-One type) to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).
- Rule 2 (One-to-One type) to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).
- Rule 3 (Many-to-One type) to map the other clients to IGA3 (200.0.0.3).
- Rule 4 (Server type) to map a web 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 map ILA to more than one IGA, therefore we must choose the **Full Feature** option from the **NAT** field in currently active remote node, and assign IGA3 to P-661H-D's WAN IP Address.

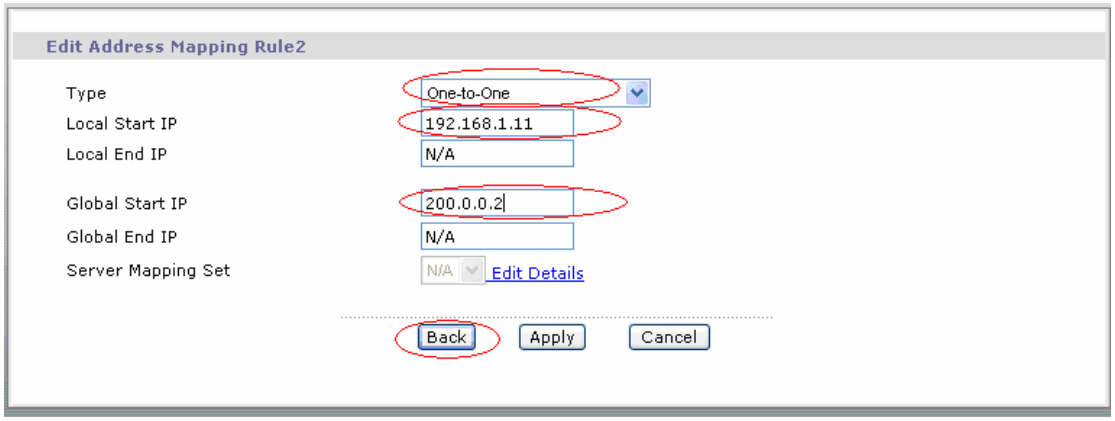



Step 2: Go to Web Configurator, Advanced Setup, **Network -> NAT -> Address Mapping** to begin configuring Address Mapping Set #1. We can see there are 10 blank rule table that could be configured. See the following setup for the four rules in our case.

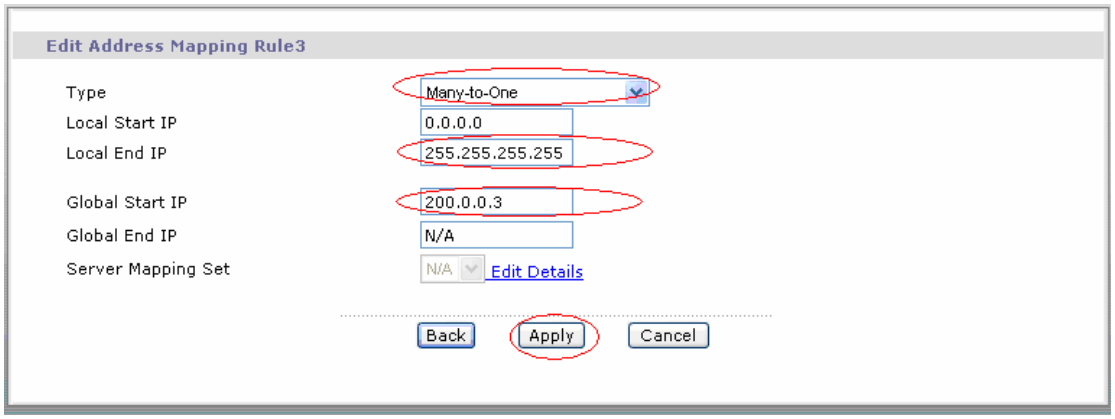
Rule 1 Setup: Select **One-to-One** type to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).



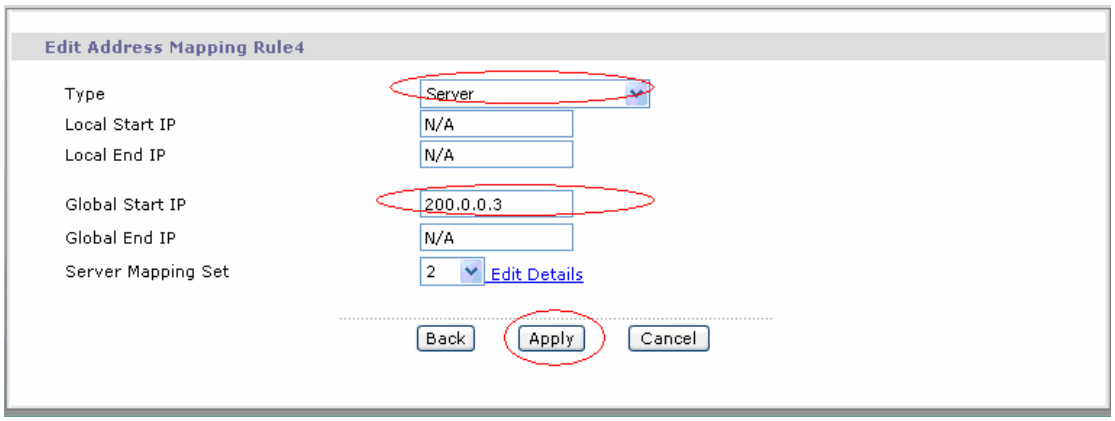

Rule 2 Setup: Selecting **One-to-One** type to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).



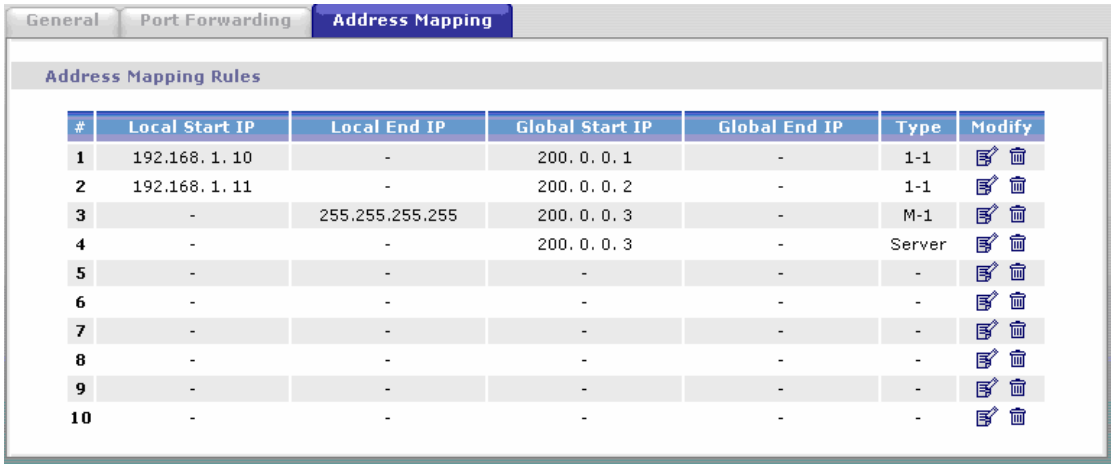

Rule 3 Setup: Select **Many-to-One** type to map the other clients to IGA3 (200.0.0.3).



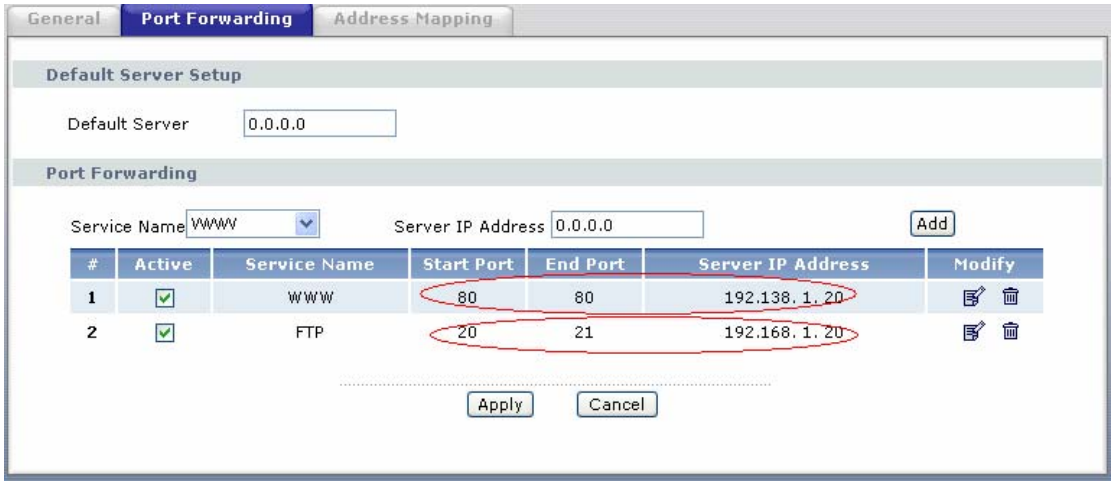

Rule 4 Setup: Select **Server type** to map our web server and mail server with ILA3 (192.168.1.20) to IGA3.




Menu **Network -> NAT -> Address Mapping** should look as follows now:

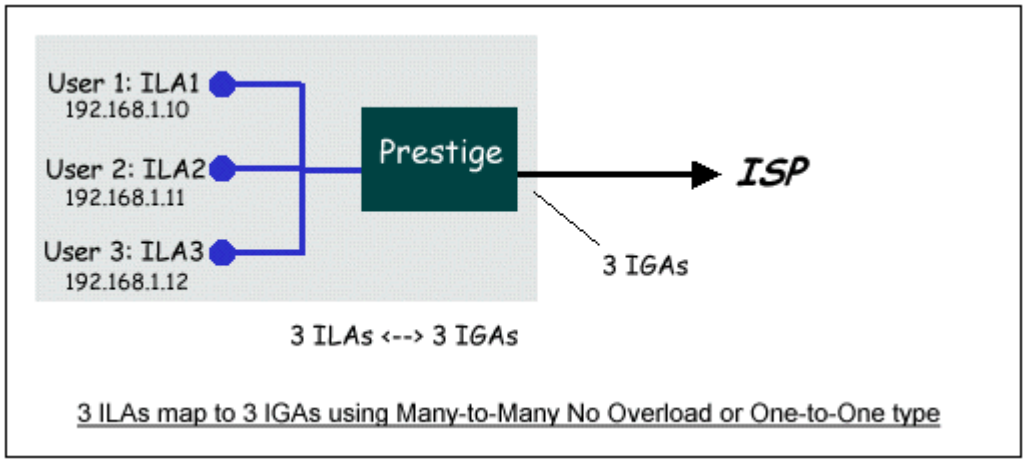



Step 3: Now we configure all other incoming traffic to go to our web server and mail server from Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding:**

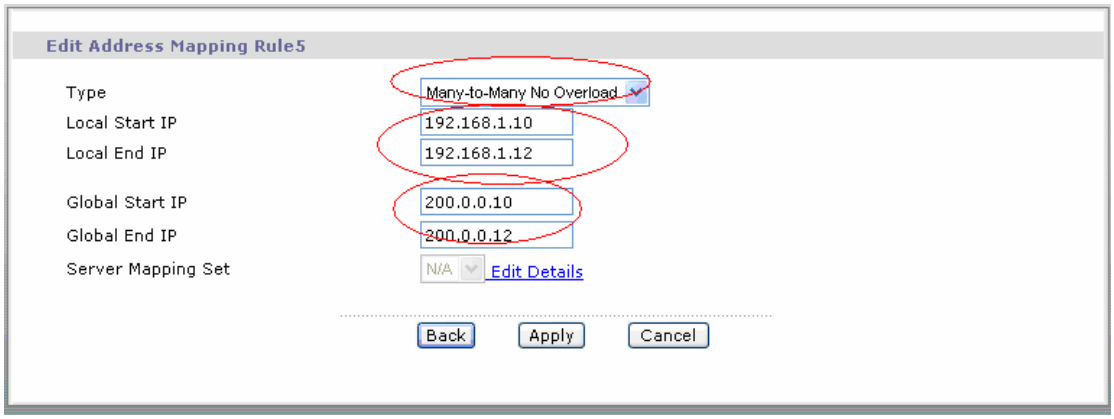



## (4) Support Non NAT Friendly Applications

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.




We can also do this by configure three**One-to-One** mapping type rules.

## 6. Using the Dynamic DNS (DDNS)

- What is DDNS?

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

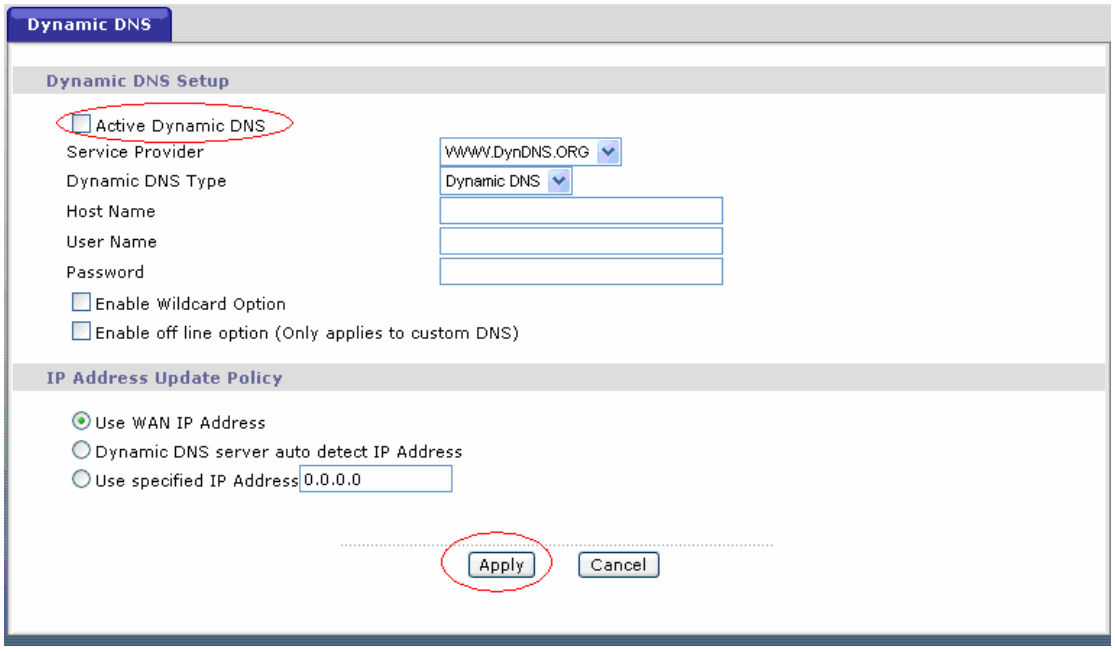
Without DDNS, we always tell the users to use the WAN IP of the P-661H-D to access the internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-661H-D, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-661H-D.

When the ISP assigns the P-661H-D a new IP, the P-661H-D 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 servers the P-661H-D supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

- Setup the DDNS

1. Before configuring the DDNS settings in the P-661H-D, 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. Login Web Configurator, Advanced Setup, **Advanced -> Dynamic DNS** Select **'Active Dynamic DNS'** option:




Key Settings:

| Option | Description |
|---|---|
| **Service Provider** | Enter the DDNS server in this field. Currently, we support WWW.DYNDNS.ORG. |
| **Active** | Toggle to **'Yes'**. |
| **Host Name** | Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw. |

| | |
|---|---|
| **User Name** | Enter the user name that the DDNS server gives to you. |
| **Password** | Enter the password that the DDNS server gives to you. |
| **Enable Wildcard** | Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is http://www.dyndns.org/. |

## 7. Network Management Using SNMP

- ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some P-661H-D routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. Further, users can also add ZyXEL's private MIB in the NMS to monitor and control additional system variables. The ZyXEL's private MIB tree is shown in figure 3. For SNMPv1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

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

1. coldStart (defined in RFC-1215) :

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

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.

(1) 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.

(2) For fatal error :
System has to reboot for some fatal errors. And traps with the message of the fatal code will be sent.

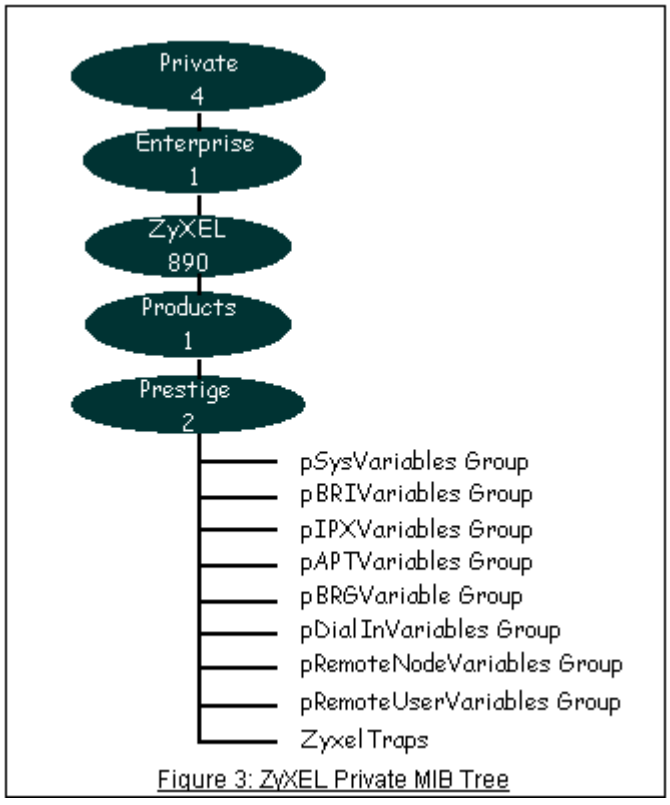
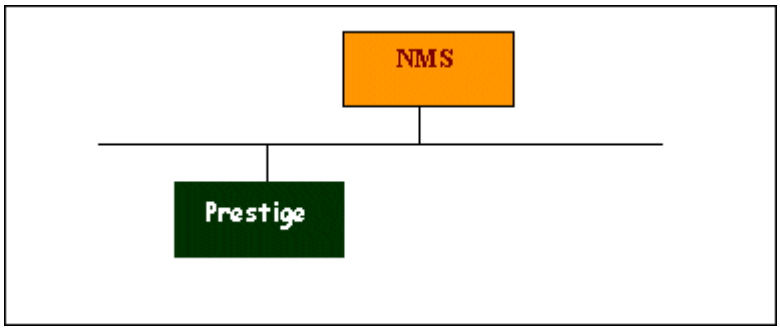
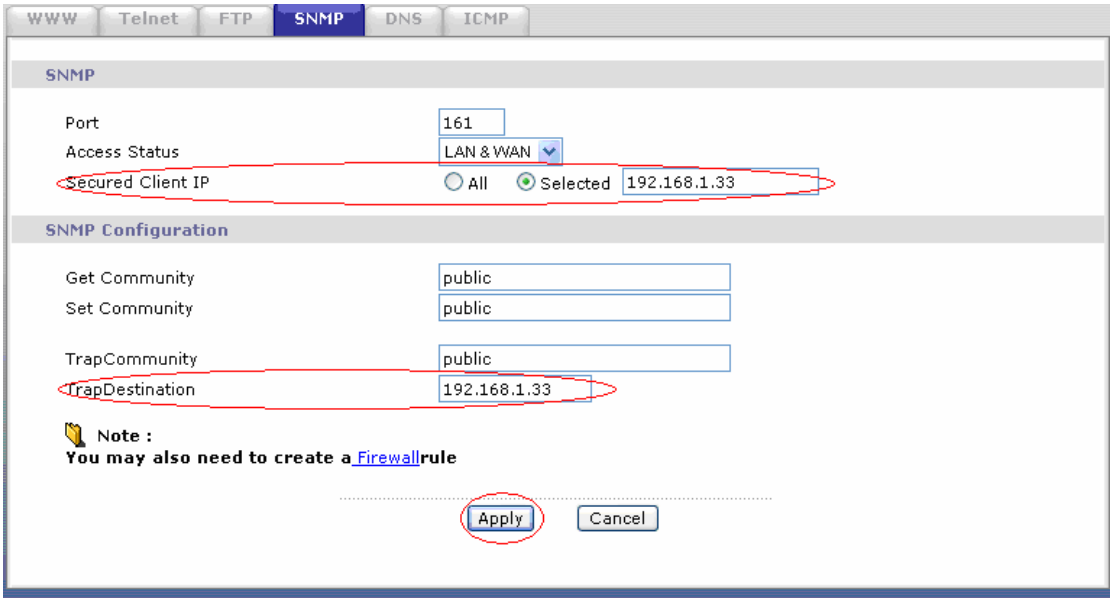


Figure 3: ZyXEL Private MIB Tree

- ***Downloading ZyXEL's private MIB***
- Configure the P-661H-D for SNMP




The SNMP related settings in P-661H-D are configured in Web Configurator, Advanced Setup, **Advanced -> Remote MGNT -> SNMP** The following steps describe a simple setup procedure for configuring all SNMP settings.



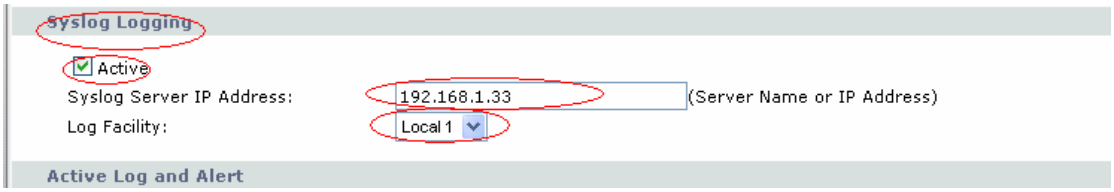

**Key Settings:**

| Option | Descriptions |
|---|---|
| **Get Community** | Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'. |
| **Set Community** | Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'. |
| **Trusted Host** | Enter the IP address of the NMS. The P-661H-DHW-DX will only respond to SNMP messages coming from this IP address. **If 0.0.0.0 is entered, the P-661H-DHW-DX will respond to all NMS managers.** |
| **Trap Community** | Enter the community name in each sent trap to the NMS. This Trap Community must match what the NMS is expecting. The default is 'public'. |

| | |
|---|---|
| **Trap Destination** | Enter the IP address of the NMS that you wish to send the traps to. **If 0.0.0.0 is entered, the P-661H-DHW-DX will not send trap any NMS manager.** |

**Note: You may need to edit a firewall rule to permit SNMP Packets.**

### 8. Using syslog



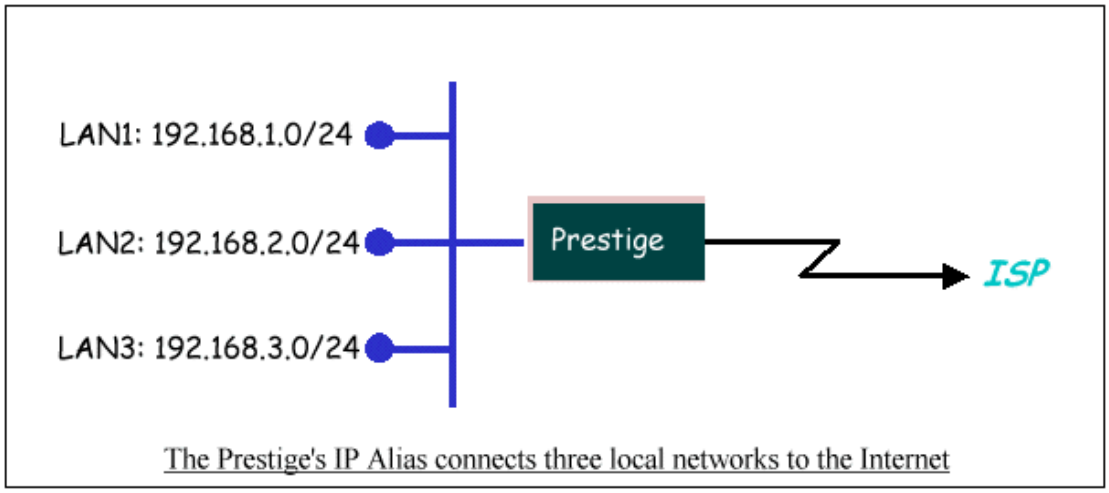

You can configure it in Web Configurator, Advanced Setup, **Maintenance -> Logs -> Log Settings -> Syslog logging.**

**Key Settings:**
**Active**: Select it to active UNIX Syslog.
**Syslog IP Address:** Enter the IP address of the UNIX server that you wish to send the syslog.
**Log Facility:** Select from the 7 different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.

### 9. Using IP Alias

- **What is IP Alias ?**

In a typical environment, a LAN router is required to connect two local networks. The P-661H-D can connect three local networks to the ISP or a remote node, we call this function as **'IP Alias'**. In this case, an internal router is not required. For example, the network manager can divide the local network into three networks and connect them to the Internet using P-661H-D's single user account. See the figure below.




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

The P-661H-D supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured in Web Configurator, Advanced Setup, **Network -> LAN -> DHCP Setup**. The second and third networks that we call **'IP Alias 1'** and **'IP Alias 2'** can be configured in **Network -> LAN -> IP Alias**.

There are three internal virtual LAN interfaces for the P-661H-D to route the packets from/to the three networks correctly. They are **enif0** for the major network, **enif0:0** for the IP alias 1 and **enif0:1** for the IP alias 2. Therefore, three routes are created in the P-661H-D as shown below when the three networks are configured. If the P-661H-D's DHCP is also enabled, the IP pool for the clients can be any of the three networks.

```
Telnet 192.168.1.1
ras> ip ro s
Dest            FF Len Device     Gateway         Metric stat Timer  Use
200.0.0.0       00 24  Idle       200.0.0.3          2    002b 0      0
192.168.1.0     00 24  enet0      192.168.1.1        1    041b 0      93
192.168.2.0     00 24  enet0      192.168.2.1        1    041b 0      0
192.168.3.0     00 24  enet0      192.168.3.1        1    041b 0      0
ras> ip if
enif0: mtu 1500
    inet 192.168.1.1, netmask 0xffffff00, broadcast 192.168.1.255
    RIP RX:None, TX:None,
    [InOctets        505058] [InUnicast      2339] [InMulticast         3220]
    [InDiscards           0] [InErrors          0] [InUnknownProtos       0]
    [OutOctets      1062338] [OutUnicast     2609] [OutMulticast         218]
    [OutDiscards          0] [OutErrors         0]
enif0:0: mtu 1500
    inet 192.168.2.1, netmask 0xffffff00, broadcast 192.168.2.255
    RIP RX:None, TX:None,
    [InOctets             0] [InUnicast         0] [InMulticast           0]
    [InDiscards           0] [InErrors          0] [InUnknownProtos       0]
    [OutOctets            0] [OutUnicast        0] [OutMulticast          0]
    [OutDiscards          0] [OutErrors         0]
enif0:1: mtu 1500
    inet 192.168.3.1, netmask 0xffffff00, broadcast 192.168.3.255
    RIP RX:None, TX:None,
    [InOctets             0] [InUnicast         0] [InMulticast           0]
    [InDiscards           0] [InErrors          0] [InUnknownProtos       0]
```

You can edit filter rule to accept or deny LAN packets from/to the IP alias 1/2 go through the P-661H-D by command in **CLI**:
**lan index [index number]**
Usage: index number =1 main LAN
2 IP Alias#1
3 IP Alias#2
**lan filter <incoming|outgoing> <tcpip|generic> [set#]**
Usage: set#= the corresponding filter set number you've configured
**lan save**

- IP Alias Setup

(1) Edit the first network in Web Configurator, Advanced Setup, **Network -> LAN -> IP/DHCP Setup** by configuring the P-661H-D's first LAN IP address.

**Key Settings:**

| | |
|---|---|
| **DHCP Setup** | If the P-661H-D's DHCP server is enabled, the IP pool for the clients can be any of the three networks. |
| **TCP/IP Setup** | Enter the first LAN IP address for the P-661H-D. This will create the first route in the enif0 interface. |

(2) Edit the second and third networks in **Network -> LAN -> IP Alias** by configuring the P-661H-D's second and third LAN IP addresses.

**Key Settings:**

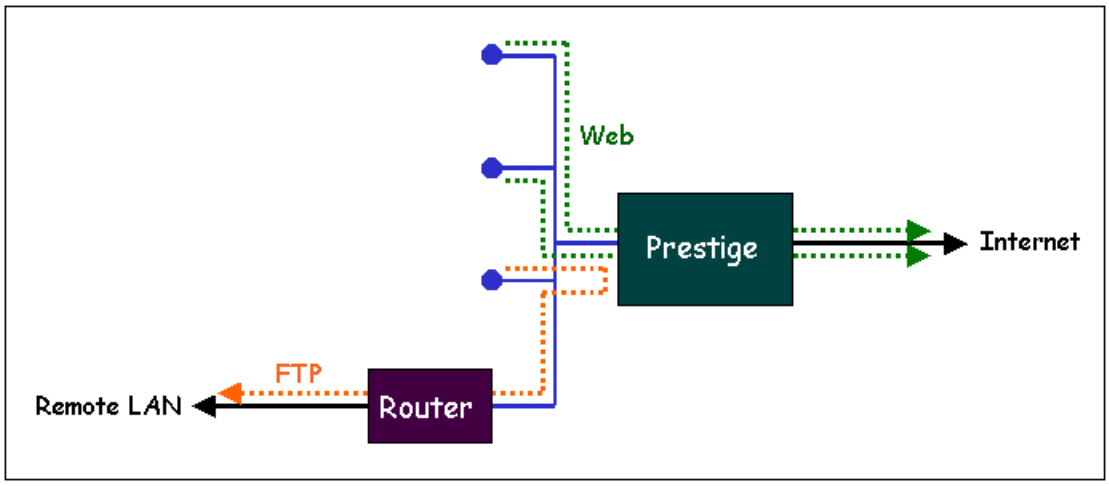
| | |
|---|---|
| **IP Alias 1** | Active it and enter the second LAN IP address for the P-661H-D. This will create the second route in the enif0:0 interface. |
| **IP Alias 2** | Active it and enter the third LAN IP address for the P-661H-D. This will create the third route in the enif0:1 interface. |

## 10. Using IP Policy Routing

- What is IP Policy Routing (IPPR)?

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

and remote node connections, we can route the Web packets to the Internet using one policy and route the FTP packets to the remote LAN using another policy. See the figure below.




Use IPPR to distribute traffic among multiple paths

- Benefits

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

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

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

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

- How does the IPPR work?

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

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

- Setup the IP Policy Routing

Setp 1: Set the index of IP routing policy set rule by command '**ip policyrouting set index [set#] [rule#]**'. Suppose set#=1, rule#=1 in this example.

Step 2: Suppose we'd like to edit the rule like this:

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

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

To implement this, we need to invoke the following command one by one:

**ip policyrouting set name Test**
(Set the name as Test of IP routing policy rule )
**ip policyrouting set active yes**
(Enable the rule)
**ip policyrouting set criteria protocol 6**

(Set the protocol ID as 6(TCP) for the rule)
**ip policyrouting set criteria serviceType 0**
(Set the criteria type of service as don't care for this rule)
**ip policyrouting set criteria precedence 8**
(Set the precedence as don't care for this rule)
**ip policyrouting set criteria packetlength 0**
(Set the packet length as 0 for the rule)
**ip policyrouting set criteria srcip 192.168.1.2 192.168.1.20**
(Set the source IP address for the rule: Start=192.168.1.2, end=192.168.1.20)
**ip policyrouting set criteria srcport 0**
(Set the source port for the rule: Start=0)
**ip policyrouting set criteria destip 0.0.0.0**
(Set the destination port for the rule: Start=0.0.0.0)
**ip policyrouting set criteria destport 80 80**
(Set the destination port for the rule: Start=80, end=80)
**ip policyrouting set action actmatched**
(Set the action for the rule: Matched)
**ip policyrouting set action gatewaytype 0**
(Set gateway type for the rule: Gateway Address)
**ip policyrouting set action gatewayaddr 192.168.1.254**
(Set the gateway address for the rule: 192.168.1.254)
**ip policyrouting set criteria serviceType 0**
(Set the action type of service as don't care for this rule)
**ip policyrouting set criteria precedence 8**
(Set the action precedence as don't care for this rule)
**ip policyrouting set action log no**
(Set log option for the rule: no log)
**ip polictrouting set save**
(Save the rule)

Step 3: Apply the IP policy routing. There are two interfaces to apply the policy set, they are the LAN interface and WAN interface. It depends where the gateway specified in the policy rule is located. If the gateway you specified is located on the local LAN you apply the policy set in LAN interface. If the gateway you specified is located on the remote WAN site you apply the policy set in WAN interface.

Apply to WAN Interface (Suppose we apply it to remote node 1 in the example):

**wan node index 1**
**wan node ippolicy 1**

## 11. Using Call Scheduling

- What is Call Scheduling?

Call scheduling enables the mechanism for the P-661H-D to run the remote node connection according to the pre-defined schedule. This feature is just like the scheduler ina video recorder which records the program according to the specified time. Users can apply at most 4 schedule sets in Remote Node. The remote node configured with the schedule set could be "Forced On", "Forced Down", "Enable Dial-On-Demand", or "Disable Dial-On-Demand" on specified date and time.

- How to configure a Call Scheduling?

You can configure a call scheduling in CLI

Suppose we want to edit a call schedule set like this:

Call Schedule Set #=1
Set name=Test
Active= Yes
Start Date(yyyy-mm-dd)= 2005 - 12 - 27
How Often= Once
Once:
Date(yyyy-mm-dd)= 2005 -12 -27
Start Time(hh:mm)= 12 : 00
Duration(hh:mm)= 16 : 00
Action= Enable Dial-on-demand

This schedule example permits a demand call on the line on 12:00 a.m., 2005-12-27. The maximum length of time this connection is allowed is 16 hours.

To implement this, we need to invoke the following command one by one:

**wan callsch index 1**
(Set call schedule index #= 1. You must apply this command first before you begin to configure call schedule)
**wan callsch name Test**
(Set the schedule name as Test)
**wan callsch active Yes**
(Enable schedule)
**wan callsch startdate 2005 12 27**
(Set schedule start date as 2005-12-27)

**wan callsch oncedate 2005 12 27**
(Set the schedule used just once, it works on 2005-12-27)
**wan callsch starttime 12 00**
(Set the schedule start time as 12:00)
**wan callsch duration 16 00**
(Set schedule duration time as 16 hours)
**wan callsch action 2**
(Set action as dial-on-demand)
**wan callsch save**
(Save the current call schedule set)

**Key Settings:**

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

- Apply the schedule to the Remote node

Multiple scheduling rules can program in a Remote node, and they have priority. For example, if we program the sets as 1,2,3,4 in remote node, then the set 1 will override set 2,3,4. set 2 will override 3,4, and so on.
We can apply the schedule to the remote node in **CLI** by the commands:

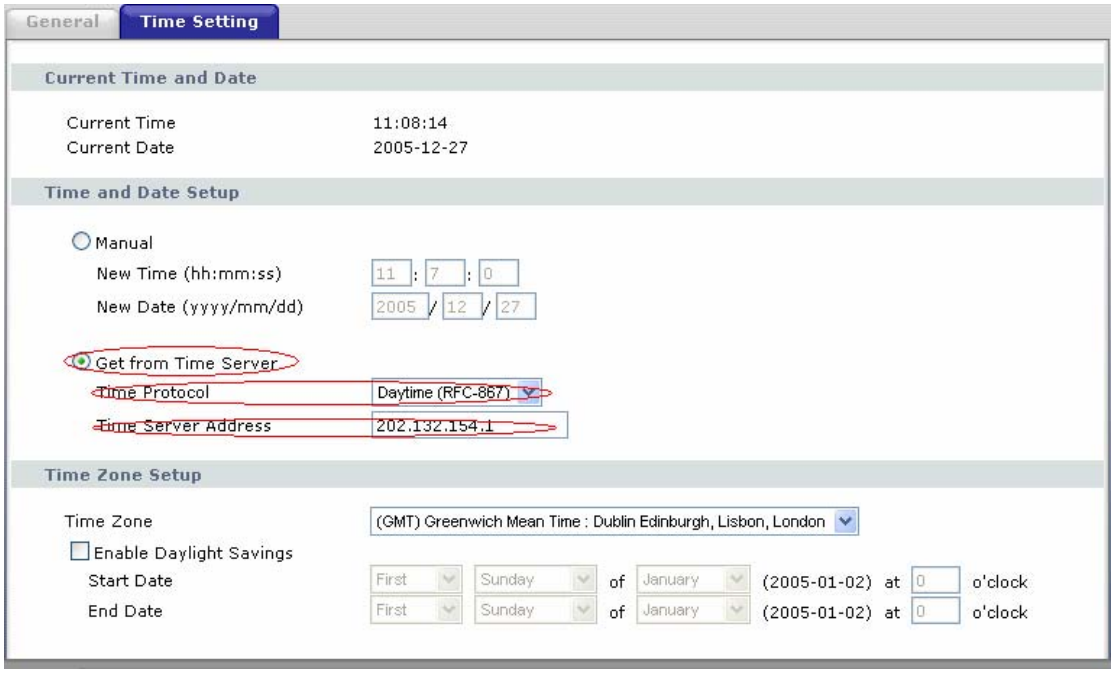
**wan node index []index#]**
**wan node callsch [index#]**
**wan node save**

For example, if we want to apply the call schedule set 1 to remote node 1, we could use the commands:

**wan node index 1**
**wan node callsch 1**
**wan node save**

- Time Service in P-661H-D

There is no RTC (Real-Time Clock) chip so the P-661H-D should launch a mechanism to get current time and date from external server in boot time. Time service is implemented by the **Daytime protocol(RFC-867)**, **Time protocol(RFC-868)**, and **NTP protocol(RFC-1305)**. You have to assign an IP address of a time server and then, the P-661H-D will get the date, time, and time-zone information from this server. You can configure it in Web Configurator, Advanced Setup, **Maintenance -> System -> Time Setting.**




## 12. Using IP Multicast

- **What is IP Multicast ?**

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

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet

needs to be forwarded. At start up, the P-661H-D queries all directly connected networks to gather group membership.

After that, the P-661H-D updates the information by periodic queries. The P-661H-D implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

- **IP Multicast Setup**

(1) Enable IGMP in P-661H-D's LAN in Web Configurator, Advanced Setup, **Network -> LAN -> IP -> Advanced Setup.**

(2) Enable IGMP in P-661H-D's remote node in Web Configurator, Advanced Setup, **Network -> Remote Node -> Edit -> Multicast.**

**Key Settings:**

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

## 13. Using Bandwidth Management

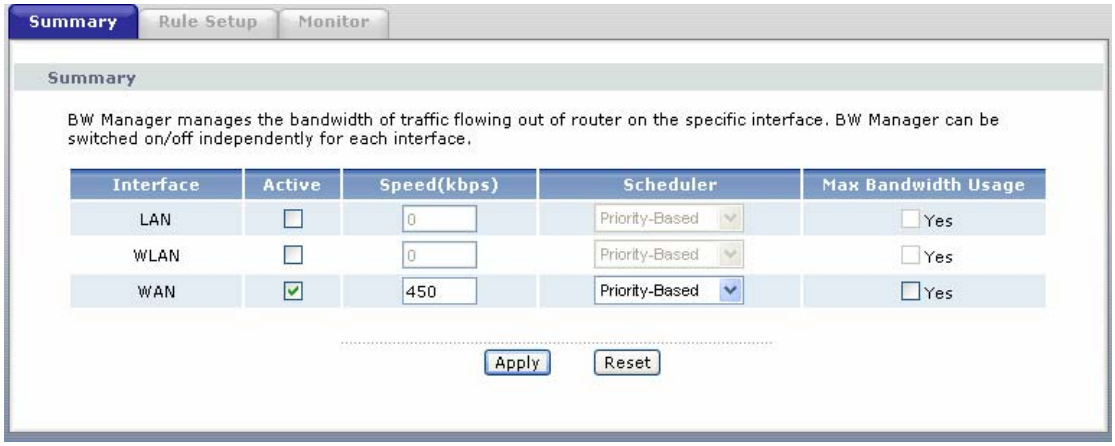
- **Why Bandwidth Management (BWM)?**

Nowadays, we have many different traffic types for Internet applications. Some traffic may consume high bandwidth, such as FTP (File Transfer Protocol). Some other traffic may not require high bandwidth, but they require stable supply of bandwidth, such as VoIP traffic. The VoIP quality would not be good, if all of the outgoing bandwidth is occupied via FTP. Additionally, chances are that you would like to grant higher bandwidth for some body specially who is using specific IP address in your network. All of these are reasons why we need bandwidth management.

- **Using BWM**

**Setp 1:** Go to Web Configurator, Advanced Setup, **Advanced -> Bandwidth MGMT->Summary**, activate bandwidth management on the interface you would like to manage. We enable the BWM function on WAN interface in this example.
Enter the total speed for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class.
Select how you want the bandwidth to be allocated. **Priority-Based** means bandwidth is allocated via priority, so the traffic with highest priority would be served first, then the second priority is served secondly and so on. If

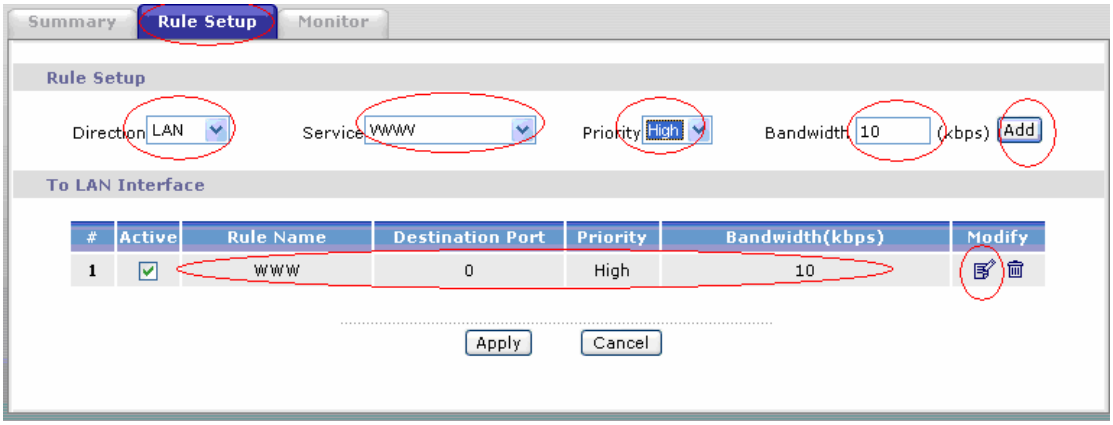
**Fairness-Based** is chosen, then the bandwidth is allocated by ratio. Which means if A class needs 300 kbps, B class needs 600 kbps, then the ratio of A and B's actual bandwidth is 1:2. So if we get 450 kbps in total, then A would get 150 kbps, B would get 300 kbps. We select **Priority-Based** in this example.



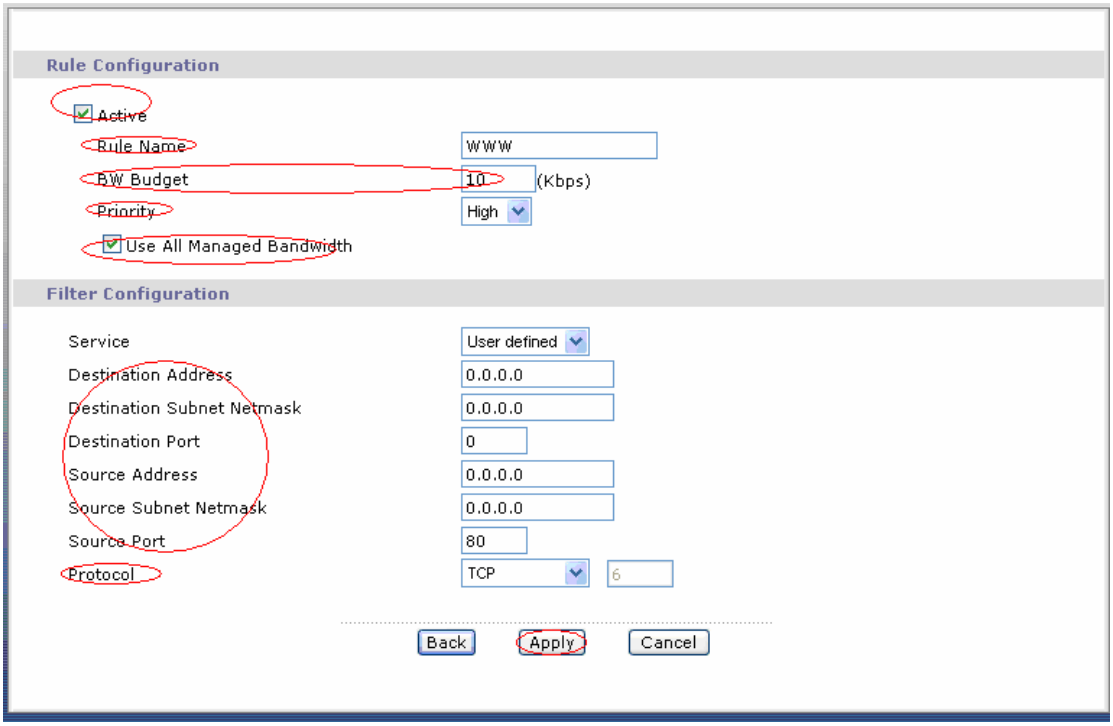

## Key Settings:

| | |
|---|---|
| **Active** | Check the box to enable BWM on the interface. Note that if you would like to manage traffic from **WAN to LAN**, you should apply BWM on **LAN** interface. If you would like to management traffic from **WAN to DMZ**, please apply BWM on **DMZ** interface. |
| **Speed** | Enter the total speed to manage on this interface. This value is the budget of the class tree's root. |
| **Scheduler** | Choose the principle to allocate bandwidth on this interface. **Priority-Based** allocates bandwidth via priority. **Fairness-Based** allocates bandwidth by ratio. |
| **Maximize Bandwidth Usage** | Check this box if you would like to give residuary bandwidth from Interface to the classes who need more bandwidth than configured amount. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the bandwidth of each class at the configured value. (Please note that to meat the second condition, you should also disable **Use All Managed Bandwidth** in the BWM rule.) |

**Step 2:** Go to Web Configurator, Advanced Setup, **Advanced -> Bandwidth MGMT-> Rule Setup**, select the **interface, Service, Priority,** and Allocated **Bandwidth** for this rule, then click button '**Add**' to apply this rule.




**Step 3**: You can modify the rule by clicking the button **'Edit'** on the rule:




## Key Settings:

| | |
|---|---|
| RuleName | Give this rule a name, for example, **'WWW'** |
| BW Budget | Configure the bandwidth you would like to allocate to this rule |
| Priority | Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3. |
| Use All Managed Bandwidth | Check this box if you would like to let this class to borrow bandwidth from it's parents when the required bandwidth is higher than the configured amount. Do not check this if you want to limit the bandwidth of this class at the configured value.(Please note that you should also disable **Maximize Bandwidth Usage** on the interface to meet the condition.) |
| Service | Select **User-defined, SIP, FTP, or H.323** to specify the traffic types |
| Destination IP Address | Enter the IP address of destination that meets this class. |

| | |
|---|---|
| Destination Subnet Mask | Enter the destination subnet mask. |
| Destination Port | Enter the destination port number of the traffic. |
| Source IP Address | Enter the IP address of source that meats this class. Note that for traffic from **'LAN to WAN'**, since BWM is before NAT, you should use the IP address before NAT processing. |
| Source Subnet Mask | Enter the destination subnet mask. |
| Source Port | Enter the source port number of the traffic. |
| Protocol ID | Enter the protocol number for the traffic. 1 for ICMP, 6 for TCP or 17 for UDP |

After configuration BWM, you can check current bandwidth of the configured traffic in Web Configurator, Advanced Setup, **Advanced -> Bandwidth MGMT-> Monitor.**

## 14. Using Zero-Configuration

- **Zero-Configuration and VC auto-hunting**

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

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

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

The entry of hunting pool must also contain the VPI, VCI, and which kinds of hunting patterns you wish to send. Whenever system send out all the probing patterns with specific VPI/VCI, system will wait for 5~10 seconds and get the response from ISP, the response patterns will decide which kinds of ADSL

services of the line will be. After that, system will save back the correct VPI, VCI and also services (encapsulation) type into profile of WAN interface.

- **Configure the VC auto-hunting preconfigured table.**

(1) Display auto-haunting preconfigured table by using command from **CLI**:

**wan atm vchunt disp**

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

(2) Add items to the auto-haunting preconfigured table by using commands:

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

**wan atm vchunt save**

**Note:** <remote node> : input the remote node index 1-8

<vpi> : vpi value

<vci> : vci value

<service>: it's a hex value, bit0:PPPoE/VC (1), bit1:PPPoE/LLC (2) , bit2:PPPoA/VC (4), bit3:PPPoA/LLC (8), bit4:Enet/VC (16), bit5 :Enet/LLC (32)

**For example:**

**(1) If you need service PPPoE/LLC and Enet/LLC then the service bits will be 2+32 = 34 (decimal) = 22 (hex), you must input 22**

**(2) If you want to enable all service for VC hunting, the service bits will be 1+2+4+8+16+32=63(decimal)= 3f (hex), you must input 3f**

Need to perform save after this by command '**wan atm vchunt save**'

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

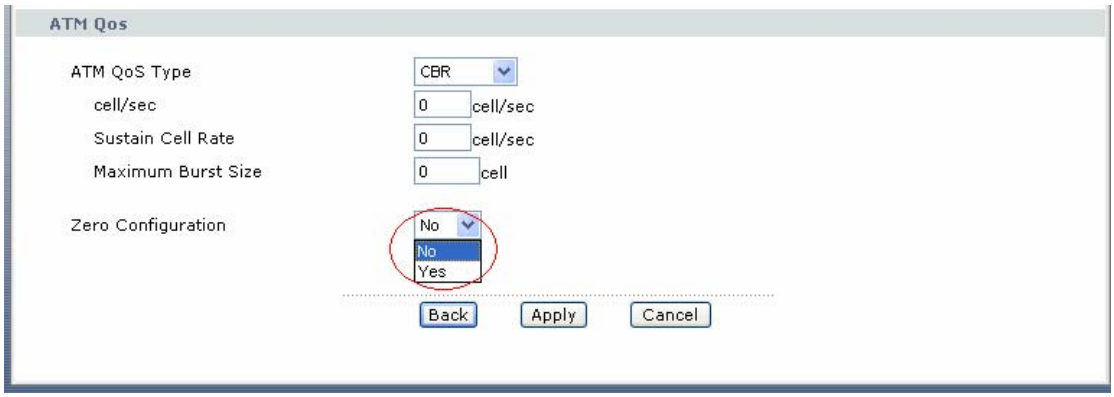
(3) Delete items from the auto-haunting preconfigured table by useing command:

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

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

- **Using Zero configuration.**

You can enable/disable Zero Configuration in **Network -> WAN -> Advanced Setup:**




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

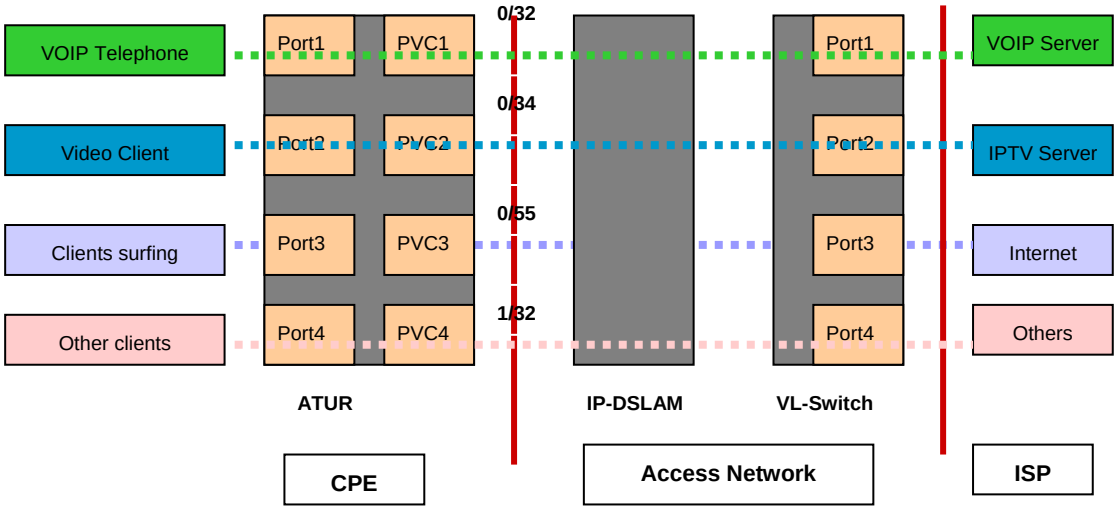
(2) Open your web browser to access a Web site. It should prompt and request for your username password of your ISP account, if your ISP provide PPPoE or PPPoA service.

(3) After key-in the correct info, it will than test the connection. If it is successful it will than close the browser and you can open a new browser to surf the Internet. If the connection test fail, it will go back to the page ask for user name and password.

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

### 15. How could I configure triple play on P-661H-D?

The common triple play scenario is as follows:




Triple Play is a port-based policy to forward packets from different LAN port to different PVCs, thus we could assign different parameters to the PVC (**CBR, UBR, VBR-RT, VBR-nRT**) to guarantee different applications.

We could configure triple play on P-661H-D via **CLI**. The command is:
**sys tripleplay set <EportID> <PVCID>**

For example: **sys tripleplay set 1 1**
**sys tripleplay set 2 2**
**sys tripleplay set 3 3**
The traffic from Ethernet port 1 must be forwarded to PVC1, vice versa.
The traffic from Ethernet port 2 must be forwarded to PVC2, vice versa.
The traffic from Ethernet Port3 must be forwarded to PVC3, vice versa.

### 16. How to configure packet filter on P-661H-D?

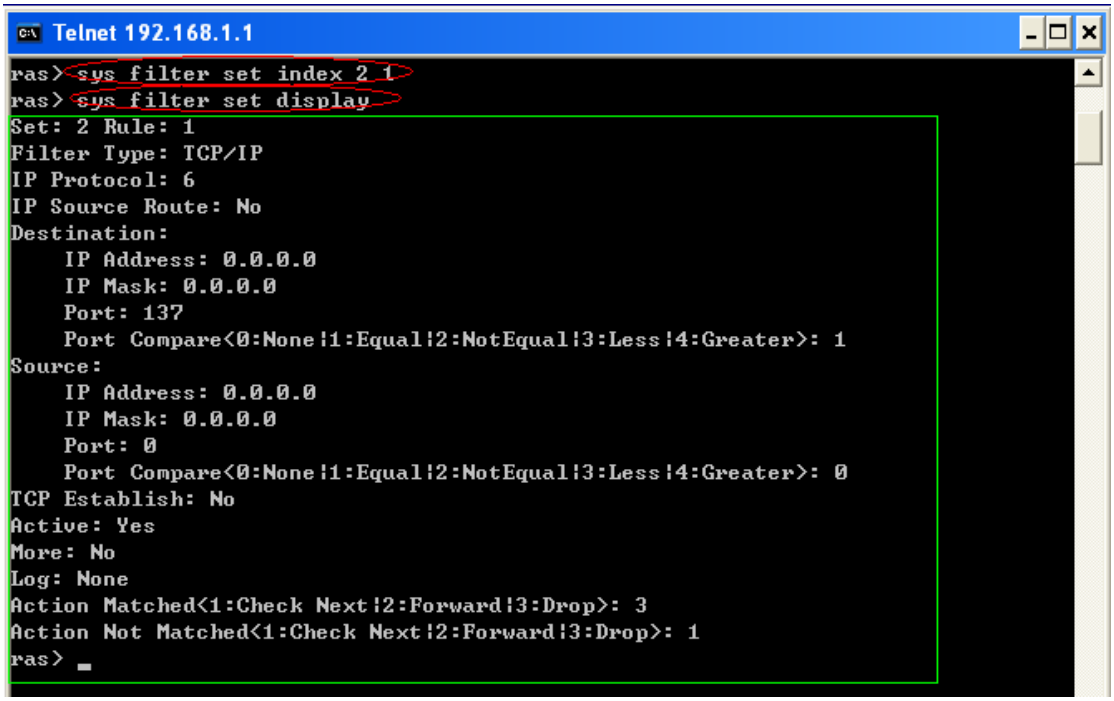
The P-661H-D allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

The packet filter function on P-661H-D is the same as before, just that you could only configure the filter set and apply them by command in **CLI.** It's very complex for common users to do it. So here's the recommendation:

(1) Usually if you want to block special packets, you could edit a firewall rule in Web Configurator.

(2) By factory default, ZyXEL has preconfigured many filter sets for your reference, you can check them by command:
**sys filter set index [set#] [rule#]**
Usage: set#: 1~12; rule#: 1~6. Commonly the preconfigured filter sets are as follows: <set 2, rule 1~6>, <set 3, rule 1>, <set 4, rule 1>.
**sys filter set display**

For example:




This could satisfy mostly requirement. You could select any of them to apply to the WAN node or LAN Interface on demand. The command is as follows:

- Apply to WAN node:

**wan node index <node#>**
Usage: node#= 1~8, corresponding to the remote node 1~8
**wan node filter <incoming|outgoing> <tcpip|generic> <set1#> <set2#> <set3#> <set4#>**
Usage: You can apply at most four filter sets to one remote node.
**wan node save**

- Apply to LAN Interface:

**lan index [index#]**
Usage: index#=1 main LAN
2 IP Alias#1
3 IP Alias#2
**lan filter <incoming|outgoing> <tcpip|generic> <set1#> <set2#> <set3#> <set4#>**
Usage: You can apply at most four filter sets to LAN Interface.
**lan save**

(3) If you are very advanced user, you could edit filter set by the following command:
**sys filter set [set#] [rule#]**
Usage: Set up a filter set index to edit a set.
set#: 1~12
rule#: 1~6
**sys filter set type [typeID]**
Usage: typeID: **tcpip** or **generic.**
Note: In one filter set, you should configure all the rules in one type: either **tcpip** or **generic.**

**sys filter set enable**
Usage: Enable(active) the rule.

**sys filter set** ……(You could configure a filter rule on demand, the newest command is available on release note)

**sys filter set save**
Usage: Don't forget to save the rule everytime you've configured it.

**Reference Commands:**

| | |
|---|---|
| sys filter set index [set#] [rule#] | Set the index of filter set rule, you must apply this command first before you begin to configure the filter rules |
| sys filter set name [set name] | Set the name of filter set |
| sys filter set type [tcpip \| generic] | Set the type of filter rule |
| sys filter set enable | Enable the rule |
| sys filter set disable | Disable the rule |
| sys filter set protocol [protocol #] | Set the protocol ID of the rule |
| sys filter set sourceroute [yes\|no] | Set the sourceroute yes/no |
| sys filter set destip [address] [subnet | Set the destination IP address and subnet mask of |

| | |
|---|---|
| mask] | the rule |
| sys filter set destport [port#] [compare type = none\|equal\|notequal\|less\|greater] | Set the destination port and compare type (compare type could be 0(none)\|1(equal)\|2(not equal)\|3(less)\|4(greater) ) |
| sys filter set srcip [address] [subnet mask] | Set the source IP address and subnet mask |
| sys filter set srcport [port#] [compare type = none\|equal\|not equal\|less\|greater] | Set the source port and compare type (compare type could be 0(none)\|1(equal)\|2(not equal)\|3(less)\|4(greater) ) |
| sys filter set tcpEstab [yes\|no] | Set TCP establish option |
| sys filter set more [yes\|no] | Set the more option to yes/no |
| sys filter set log [type 0-3= none \| match\| notmatch \| both ] | Set the log type (it could be 0-3 =none, match, not match, both) |
| sys filter set actmatch[type 0-2 = checknext \| forward \| drop] | Set the action for match |
| sys filter set actnomatch [type 0-2 = checknext \| forward \| drop] | Set the action for not match |
| sys filter set offset [#] | Set offset for the generic rule |
| sys filter set length [#] | Set the length for generic rule |
| sys filter set mask [#] | Set the mask for generic rule |
| sys filter set value [(depend on length in hex)] | Set the value for generic rule |
| sys filter set clear | Clear the current filter set |
| sys filter set save | Save the filter set parameters |
| sys filter set display [set#][rule#] | Display Filter set information. W/o parameter, it will display buffer information. |
| sys filter set freememory | Discard Changes |

# IPSEC VPN Application Notes

### 1. How to use P-661H-D to build VPN Tunnel with another VPN Gateway/ Software?

This page will guide you to setup a VPN connection between two Prestige routers. In addition to Prestige to Prestige, Prestige can also talk to other VPN hardwards/softwares. The tested VPN hardwares 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 VPN solution
- Avaya VPN
- Netopia VPN
- III VPN

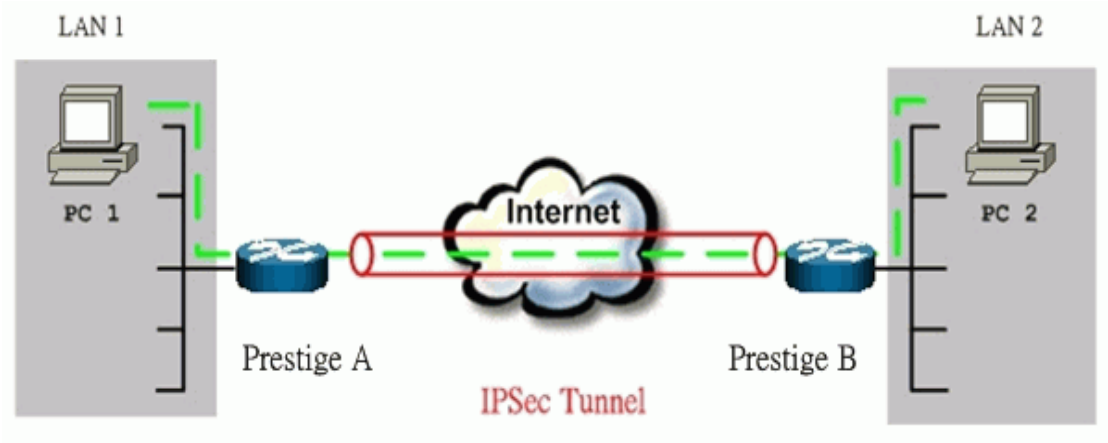
The tested VPN softwares are shown below:

- Checkpoint VPN software
- WIN2K VPN software
- Soft-PK VPN software
- Linux FreeS/WAN VPN
- SSH Sentinel
- Intel VPN client software

Let's focus on the how to configure VPN tunnel on Prestige now:

- **Prestige to Prestige Tunnel**

As the figure shown below, the tunnel between Prestige 1 and Prestige 2 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 Prestige are explained in the following sections.




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

| PC 1 | Prestige A | Prestige B | PC 2 |
|---|---|---|---|
| 192.168.1.33 | LAN: 192.168.1.1<br>WAN: 202.132.154.1 | LAN: 192.168.2.1<br>WAN: 168.10.10.66 | 192.168.2.33 |

**Note:** 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. If both of VPN gateways use dynamic IP, we need DDNS service to implement it.

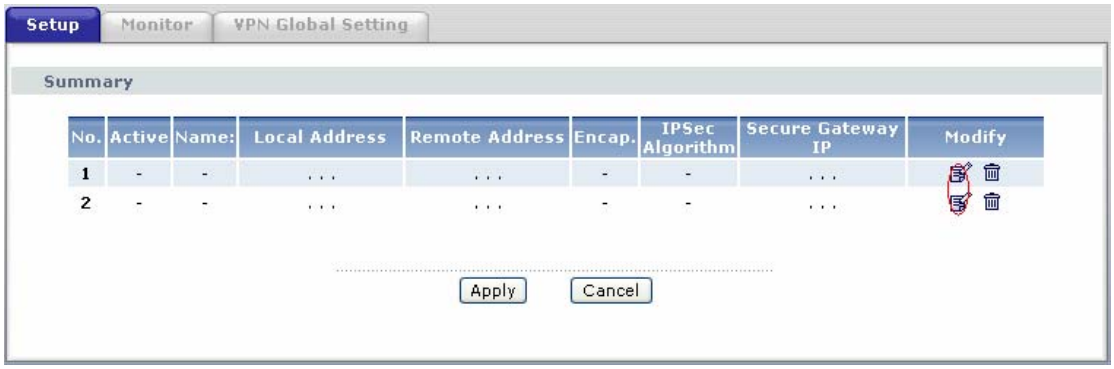
You can finish the configuration via Web Configurator on Prestige:

**Step 1: Set up Prestige A**

(1) Using a web browser, login Prestige Web Configurator by giving the LAN IP address of Prestige in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.

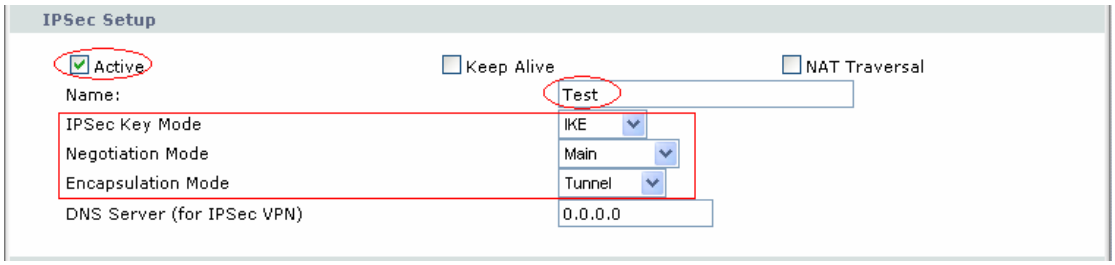
Note: For P-661H-D, you need to login Multilingual Web Configurator using Administrator account, the default password is **admin**

(2) Go to VPN Setup page to edit a VPN Rule. On P-661H-D, you could begin with **Security -> VPN -> Summery:**



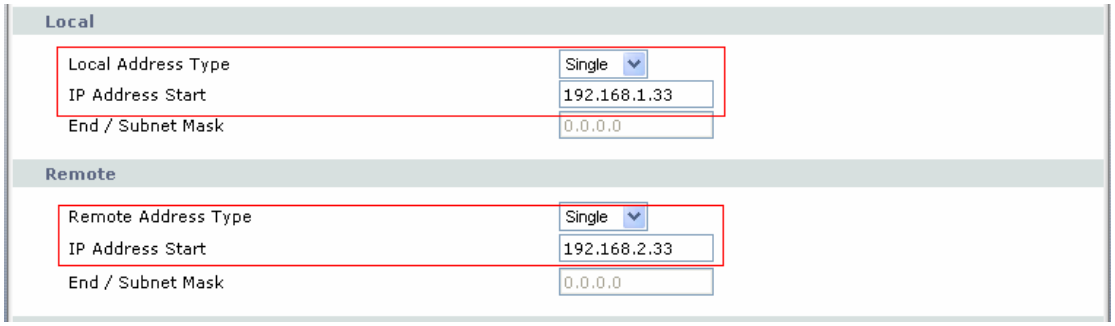

(3) On the **SUMMARY** menu, select a policy to edit by clicking **Edit**. On P-661H-D, we can build at most 2 VPN Tunnels. Just make a click on the '**Edit**' button in the table, we can begin to configure the VPN rule.

(4) In the **IPSEC Setup** field, toggle **Active** check box and give a name, **Test** in the example to this policy.
Select **IPSec Key Mode** to **IKE, Negotiation Mode** to **Main**, and **Encapsulation Mode** to **Tunnel**, just the same as we will configure in Prestige B.



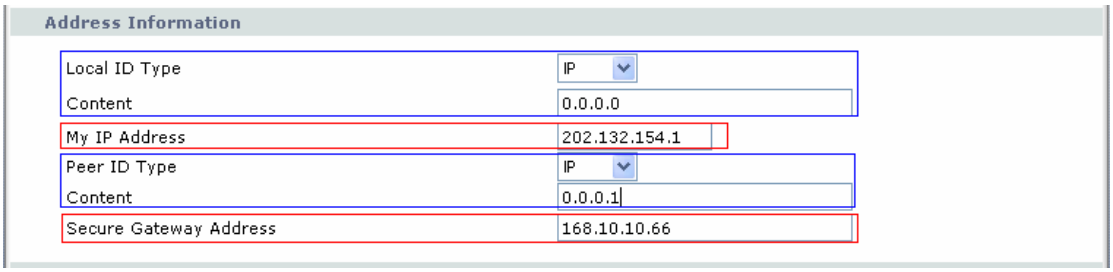

(5) Fill in the Local and Remote secure hosts information in the **Local** and **Remote** field.

**Local Address Type** is **Single** and **IP Address Start** is **PC 1's IP**, **192.168.1.33** in the example.
**Remote Address Type** is **Single** and **IP Address Start** is **PC 2's IP**, **192.168.2.33** in the example.



(6) Fill in the VPN Gateway information in the **Address Information** field.

**My IP Address** is the **WAN IP of Prestige A**, **202.132.154.1** in the example.
**Secure Gateway Address** is the remote secure gateway, **Prestige B's WAN IP**, **168.10.10.66** in the example.
**Local ID Type** as **IP**, and **Content** as **0.0.0.0** in the example.
**Peer ID Type** as **IP**, and **Content** as **0.0.0.1** in the example.

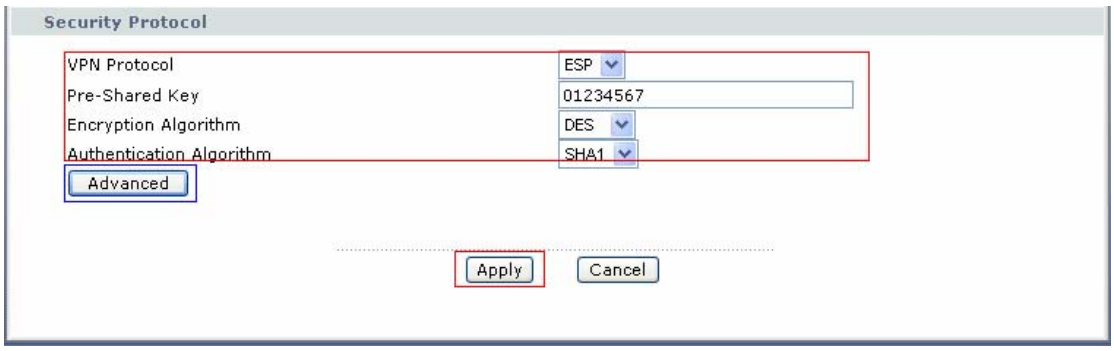



Note: Make sure the ID Type and content consistent between the two VPN secure gateways. As in the example, we've finished this field on Prestige A, then when we configure Prestige B, we should make it fit the following table:

| | Prestgie A | Prestige B |
|---|---|---|
| Local ID Type | IP | IP |
| Content | 0.0.0.0 | 0.0.0.1 |
| Peer ID Type | IP | IP |
| Content | 0.0.0.1 | 0.0.0.0 |

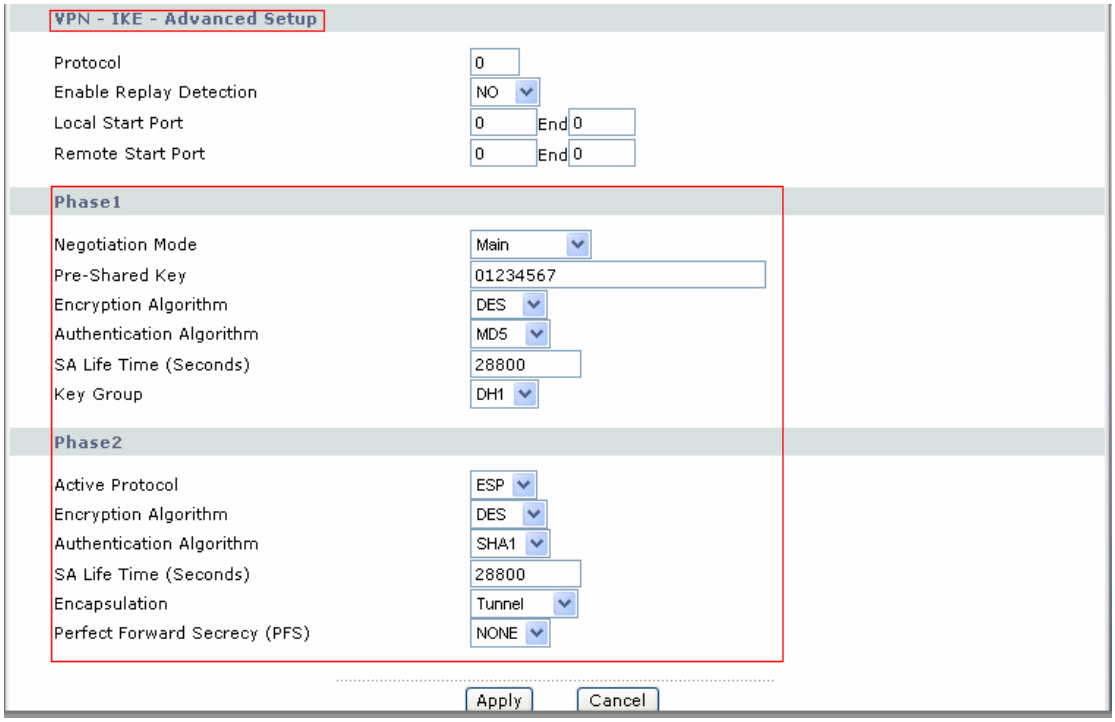
(7) Fill in VPN Protocol, Pre-Shared Key, Encryption Algorithm, Authentication Algorithm in the **Security Protocol** field

Select one **VPN Protocol** from the pull-down menu, **ESP** in the example.
Input a proper **Pre-Shared Key** in the right table, 01234567 in the example.
Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**.



Note: If there's a NAT router between the two VPN Secure Gateways, we should only choose '**ESP**' VPN Protocol
The minimum length of **Pre-Shared Key** is **8**.

(8) A common VPN Rule has been completed, you can click 'Apply' to save it. But if you want to make more special configuration, you could click 'Advanced' to continue:




Note: If you make any change in advanced setup, you need to configure the same on Prestige B.

We don't do any anvanced setup in the example. Then we have finished the configuration on Preatige A.

**Step 2: Setup Prestige B**

Similar to the settings for Prestige A, Prestige B is configured in the same way except that:
(1) **Local Address Type** is **Single** and **IP Address Start** is **PC 2's IP**, **192.168.2.33** in the example.
**Remote Address Type** is **Single** and **IP Address Start** is **PC 1's IP**, **192.168.1.33** in the example.

(2) **My IP Address** is the **WAN IP of Prestige B**, **168.10.10.66** in the example.

**Secure Gateway Address** is the remote secure gateway, **Prestige A's WAN IP**, **202.132.154.1** in the example.

(3) **Local ID Type /Content** should be the same as **Prestige A's Peer ID Type/Content**, **IP/0.0.0.1** in the example.
**Peer ID Type** /**Content** should be the same as **Prestige A's Local ID Type/ Content**, **IP/0.0.0.0** in the example.

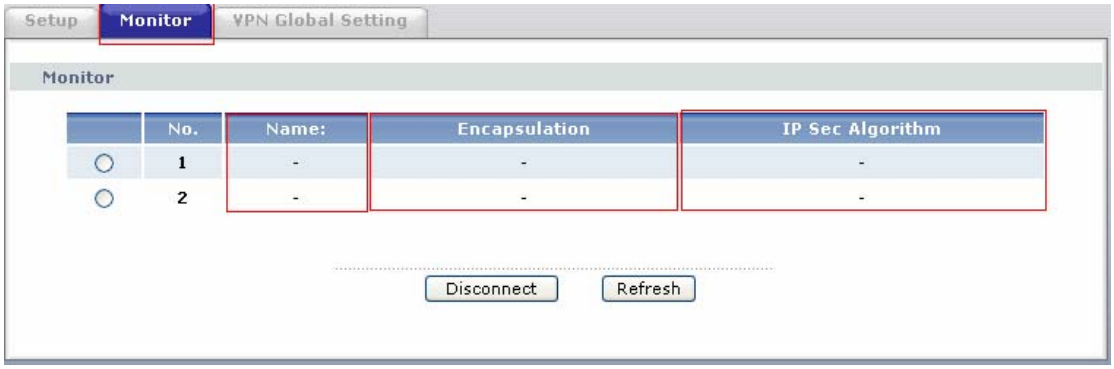
**Step 3: Verify if the VPN Tunnel has been established successfully**

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 ( ping **192.168.2.33** or **192.168.1.33** in the example ), it means that the IPSec tunnel has been established successfully. If the ping fail, there are two methods to troubleshoot IPSec in Prestige:

(1) Check the VPN Monitor

On P-661H-D Web Configurator, **Security -> VPN -> Monitor,** you can check every active IPSec connections. The VPN Name, Encapsulation, and IPSec Algorithm will be shown in the Monitor Table.If you can't see the name of your IPSec rule, it means that the SA establishment fails. You need to go to the VPN Setup Page to check your settings.



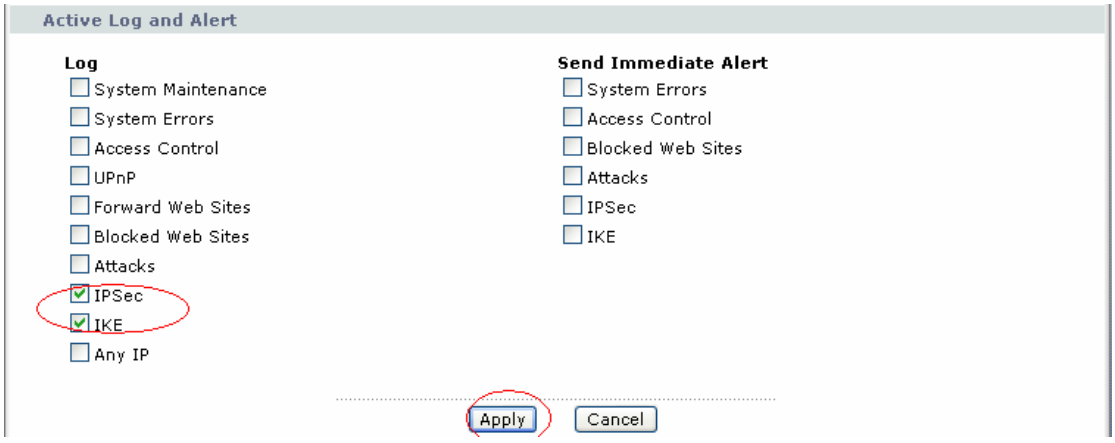

- Use CI command **'ipsec debug on'**

If the Monitor shows that the VPN tunnel has been established successfully, but the PC1 and PC 2 can't reach each other. We can invoke command '**ipsec debug 1**' in CLI for trouble shooting. 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' and send the dump information to Support Engineer for a solution. The following shows an example of dumped messages. (You can refer to Support Tool -> 1 WAN/ LAN Packet Trace -> Capture the detailed logs by Hyper Terminal to do it).

Prestige> ipsec debug 1
IPSEC debug level 1
Prestige> 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

### (2) View IPSec Log

We can also view the log for IPSec and IKE connections for trouble shooting. On P-661H-D, we can check the logs via **Web Configurator** or **CLI**. The log menu is also useful for troubleshooting please capture to us if necessary. For example: Select **IPSec** and **IKE** in Web Configurator, **Maintenance -> Logs -> Log Settings**




Then after a successful or failed VPN connection, we could view the relevant information from Web Configurator, **Maintenance -> Logs -> View Log:**


### 2. How to build a VPN between Secure Gateway with Dynamic WAN IP Address?

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 be predefined in the VPN box. There are some tips when configure Prestige in any dynamic case.

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

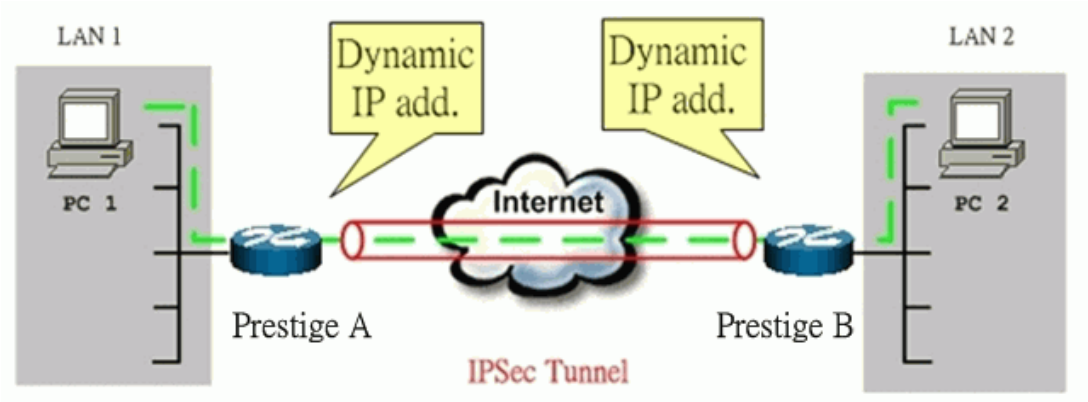
We need to note:
(1) In VPN settings of Prestige, please specify the IP address of **Secure Gateway** as **0.0.0.0**
(2) The VPN connection can **ONLY** be initiated from dynamic side to static side in order to update its dynamic IP to the static side.
(3) In peer side, are you using **Win2K built-in 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.

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

We need to note:
(1) In VPN settings of Prestige, please specify the IP address of **My IP** as **0.0.0.0**. Prestige will automatically bind it's current WAN IP address to IPSec.
(2) IPSec tunnel in this case, can **ONLY** be initiated from Prestige.
(3) In peer side, are you using **SonicWALL, NetScreen?** SonicWALL requires you to enter an ID (in FQDN format) to identify Prestige.

- **Prestige dynamic WAN IP v.s. peer side dynamic IP**

In this case, we need to use DDNS (Dynamic Domain Name Service). There are many different solutions for it:
**(1) Prestige v.s. Prestige**




**Solution 1:**

Step 1: In Prestige A, please register a DDNS account from http://www.dyndns.org or http://dynupdate.no-ip.com

Setp 2: Enable **DynDNS** function on Prestige A via Web configurator, **Advanced -> Dynamic DNS**. And in VPN settings on Prestige A, please specify the IP address of **My IP** as **0.0.0.0** and **Secure Gateway** as **0.0.0.0** (Here we take P-661H-D Web Configurator as the example).

Step 3: In Prestige B, please specify the IP address of **My IP** as **0.0.0.0** and **Secure Gateway** as the domain name you registered for Prestige A.

Step 4: Please always initiate VPN tunnel from Prestige B on which Secure Gateway is configured as dynamic domain name.

**Solution 2:**

Step 1: Register DynDNS account from http://www.dyndns.org or http://dynupdate.no-ip.com for both PrestigeA & PrestigeB.

Step 2: In PrestigeA, configure **My IP** as **0.0.0.0** and **Secure Gateway** as the dynamic domain name of PrestigeB.

Step 3: In PrestigeB, configure **My IP** as **0.0.0.0** and **Secure Gateway** as the dynamic domain name of PrestigeA.

Step 4: You can initiate VPN tunnel from PrestigeA or PrestigeB by this solution.

**(2) Prestige v.s. 3rd Party**

This is highly dependent on which kind of 3rd party you use. Generally speaking, this 3rd party VPN solution must support either of the two items:

- Support DDNS for update of it's dynamic WAN IP. (If Prestige is to be the VPN initiator)
- Support Secure Gateway can be configured by Domain Name. (If Prestige is to be the VPN responder)

**3. 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 Prestige, 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.

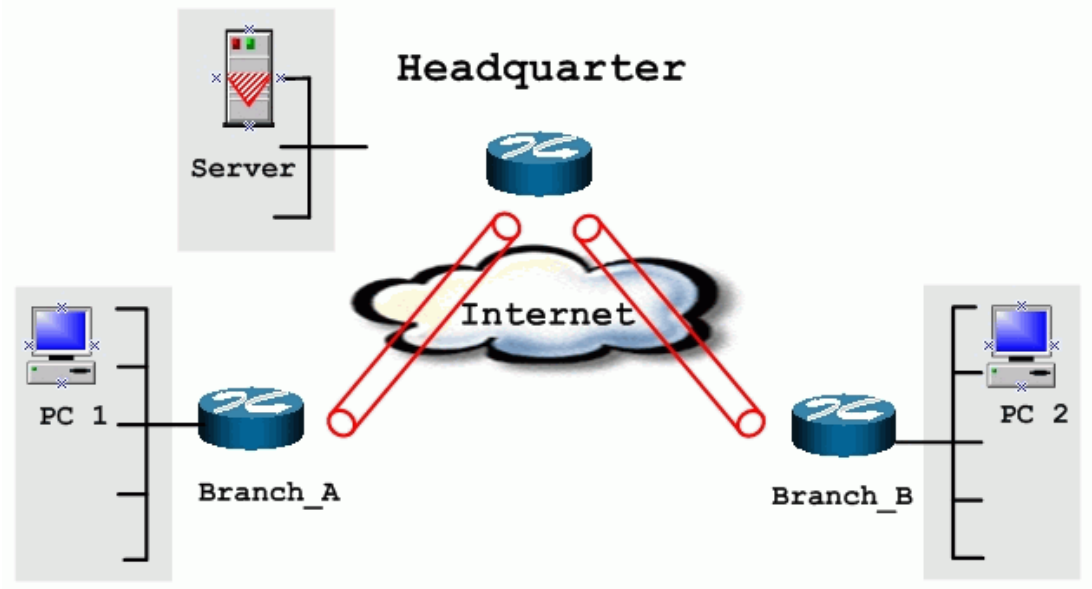
For example:

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

### 4. VPN Routing between Branch Office through Headquarter

This page guides us how to setup VPN routing between branch offices through headquarter. So that whenever branch office A wants to talk to branch office B, headquarter plays as a VPN relay. Users can gain benefit from such application when the scale of branch offices is very large, because no additional VPN tunnels between branch offices are needed. In this support note, we skip the detailed configuration steps for Internet access and presume that you are familiar with basic ZyNOS VPN configuration.

As the figure shown below, each branch office have a VPN tunnel to headquarter, thus PCs in branch offices can access systems in headquarter via the tunnel. Through VPN routing, Prestige series now provide you a solution to let PCs in branch offices talk to each other through the existing VPN tunnels concentrated on the headquarter.



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

| Branch_A | Headquarter | Branch_B |
|---|---|---|
| WAN:202.3.1.1<br>LAN:192.168.3.1 | WAN:202.1.1.1<br>LAN:192.168.1.1 | WAN:202.2.1.1<br>LAN:192.168.2.1 |
| **LAN of Branch_A** | **LAN of Headquarter** | **LAN of Branch_B** |
| 192.168.3.0/24 | 192.168.1.0/24 | 192.168.2.0/24 |

**Setp 1: Setup VPN in branch office A**

Because VPN routing enables branch offices to talk to each other via tunnels concentrated on headquarter. In this step, we configure an IPSec rule in Prestige (Branch_A) for PCs behind branch office A to access both LAN segments of headquarter and branch office B. Because the LAN segments of headquarter and branch office B are continuous, we merge them into one single rule by including these two segments in **Remote** section. If by any chance, the two segments are not continuous, we strongly recommend you to setup different rules for these segments.

Create a VPN Rule with name **Branch_A**. The configuration is the same as Prestige to Prestige Tunnel, just the IP Address is a little different:

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.3.0, IP Address End** is **192.168.3.255.** This section covers the LAN segment of branch office A.

**Remote Address Type** is **Range Address** and **IP Address Start** is **192.168.1.0**, IP Address End is **192.168.2.255**. This section covers the LAN segment of both headquarter and branch office B.

(2) **My IP Address** is the WAN IP of Prestige in **Branch_A**, **202.3.1.1** in the example.
**Secure Gateway Address** is **IP address of Headquarter**, **202.1.1.1** in the example.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don’t make any advanced setup in the example.

**Step 2: Setup VPN in branch office B**

Be very careful about the remote IP address in branch office B, because systems behind branch office B want to access systems behind branch office A and headquarter, we have to specify these two segments in **Remote** section. However if we include these two segments in one rule, the LAN segment of branch office B will be also included in this single rule, which means intercommunication inside branch office B will run into VPN tunnel. To avoid such situation, we need two separate rules to cover the LAN segment of branch office A and headquarter.

- **The first rule in Branch_ B, Branch_B_1.**

This rule is for branch office B to access headquarter.

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.2.0, IP Address End** is **192.168.2.255.** This section covers the LAN segment of branch office B.

**Remote Address Type** is **Range Address** and **IP Address Start** is **192.168.1.0**, IP Address End is **192.168.1.255**. This section covers the LAN segment of headquarter office.

(2) **My IP Address** is the WAN IP of Prestige in **Branch_B**, **202.2.1.1** in the example.
**Secure Gateway Address** is **IP address of Headquarter**, **202.1.1.1** in the example.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don’t make any advanced setup in the example.

- **The second rule in Branch_B, Branch_B_2.**

This rule is for branch office B to access branch office A.

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.2.0, IP Address End** is **192.168.2.255.** This section covers the LAN segment of branch office B.

**Remote Address Type** is **Range Address** and **IP Address Start** is **192.168.3.0**, IP Address End is **192.168.3.255**. This section covers the LAN segment of branch office A.

(2) **My IP Address** is the WAN IP of Prestige in **Branch_B**, **202.2.1.1** in the example.
**Secure Gateway Address** is **IP address of Headquarter**, **202.1.1.1** in the example.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don't make any advanced setup in the example.

**Step 3: Setup VPN in Headquarter**

- **The corresponding rule for Branch_A in headquarter**

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.1.0, IP Address End** is **192.168.1.255.** This section covers the LAN segment of Headquarter office.

**Remote Address Type** is **Range Address** and **IP Address Start** is **192.168.3.0**, IP Address End is **192.168.3.255**. This section covers the LAN segment of branch office A.

(2) **My IP Address** is the **IP Address of Headquarter**, **202.1.1.1** in the example.
**Secure Gateway Address** is WAN IP of Prestige in **Branch_A**, **202.3.1.1** in the example.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don't make any advanced setup in the example.

- **The correspondent rule for Branch_B_1 in headquarter**

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.1.0, IP Address End** is **192.168.1.255.** This section covers the LAN segment of Headquarter office.

**Remote Address Type** is **Range Address** and **IP Address Start** is **192.168.2.0**, IP Address End is **192.168.2.255**. This section covers the LAN segment of branch office B.

(2) **My IP Address** is the **IP Address of Headquarter**, **202.1.1.1** in the example.
**Secure Gateway Address** is WAN IP of Prestige in **Branch_B**, **202.2.1.1** in the example.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don't make any advanced setup in the example.

- **The correspondent rule for Branch_B_2 in headquarter**

(1) **Local Address Type** is **Range Address** and **IP Address Start** is **192.168.3.0, IP Address End** is **192.168.3.255.** This section covers the LAN segment of branch office A.

**Remote Address Type** is **Range Address** and **IP Address Start** is **192.168.2.0**, IP Address End is **192.168.2.255**. This section covers the LAN segment of branch office B.

(2) **My IP Address** is the **IP Address of Headquarter**, **202.1.1.1** in the example.
**Secure Gateway Address** is WAN IP of Prestige in **Branch_B**, **202.2.1.1** in the example.

(3) Suppose the pre-shared key is **01234567**, we should configure the same key in the corresponding rule in Headquarter VPN Gateway.

(4) You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the corresponding VPN rule in headquarter. We don't make any advanced setup in the example.

# Support Tool

### 1. LAN/WAN Packet Trace

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

The format of the display is as following:

Packet:


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

There are two ways to dump the trace:

**Online Trace**--display the trace real time on screen

**Offline Trace**--capture the trace first and display later

**The details for capturing the trace in CLI as follows:**

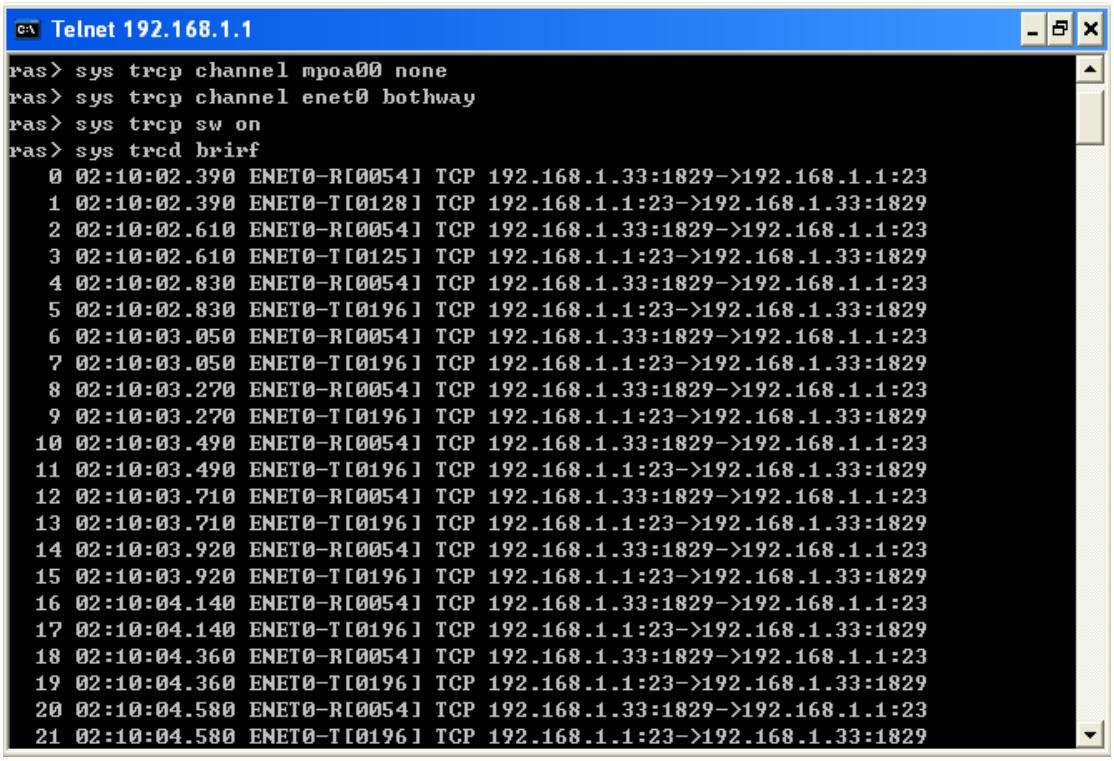
First of all, you need to telnet to the P-661H-D firstly. The password is Administrator passwords, ‘admin’ by default.

- **Online Trace**

(1) Trace LAN packet

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

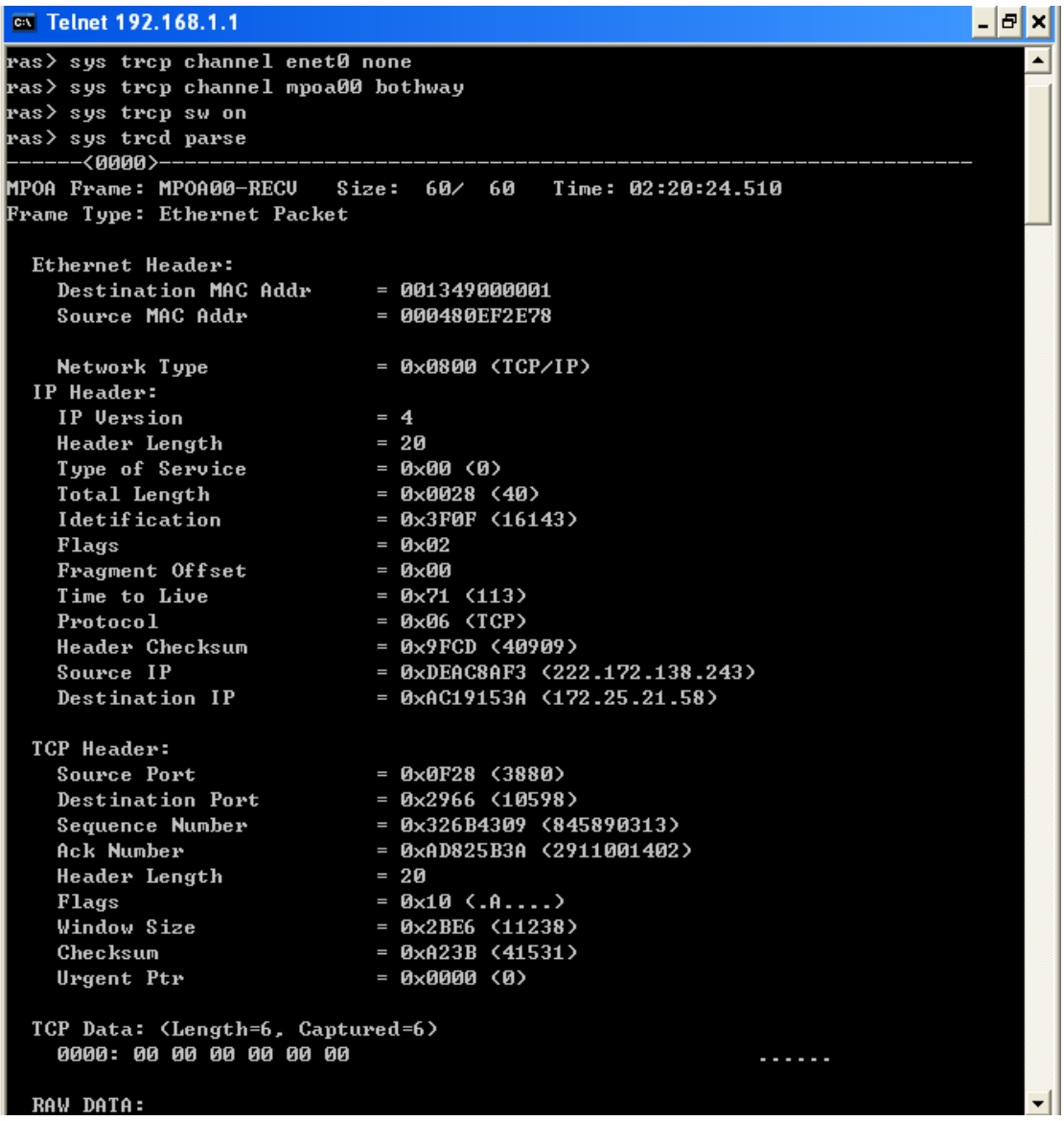
**Example:**




(2) Trace WAN packet

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

**Example:**

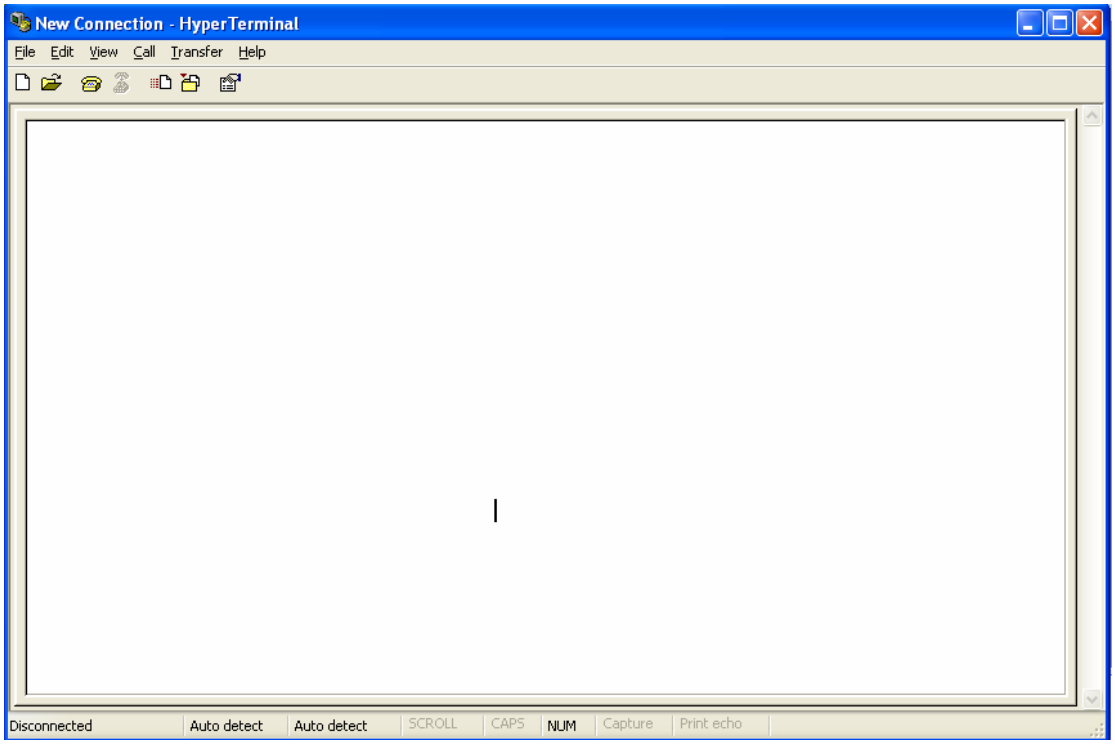



- **Offline Trace**

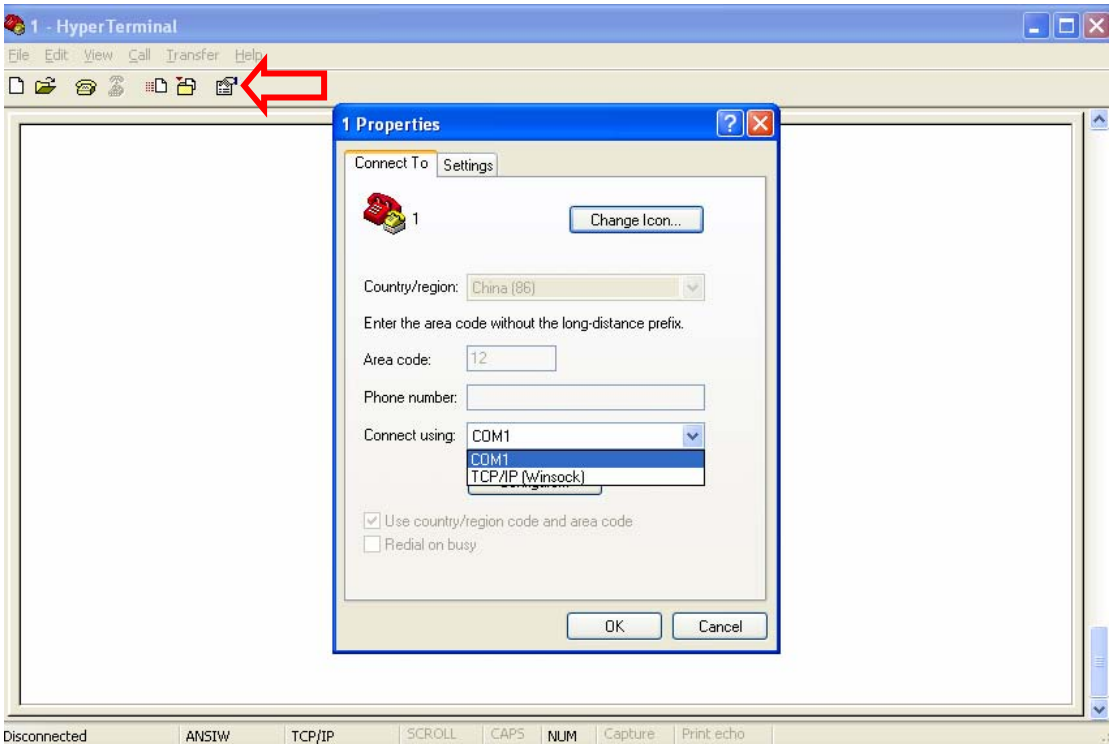
- Disable the capture of the WAN packet by entering: **sys trcp channel mpoa00 none**
- Enable the capture of the LAN packet by entering: **sys trcp channel enet0 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Wait for packet passing through the Prestige over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

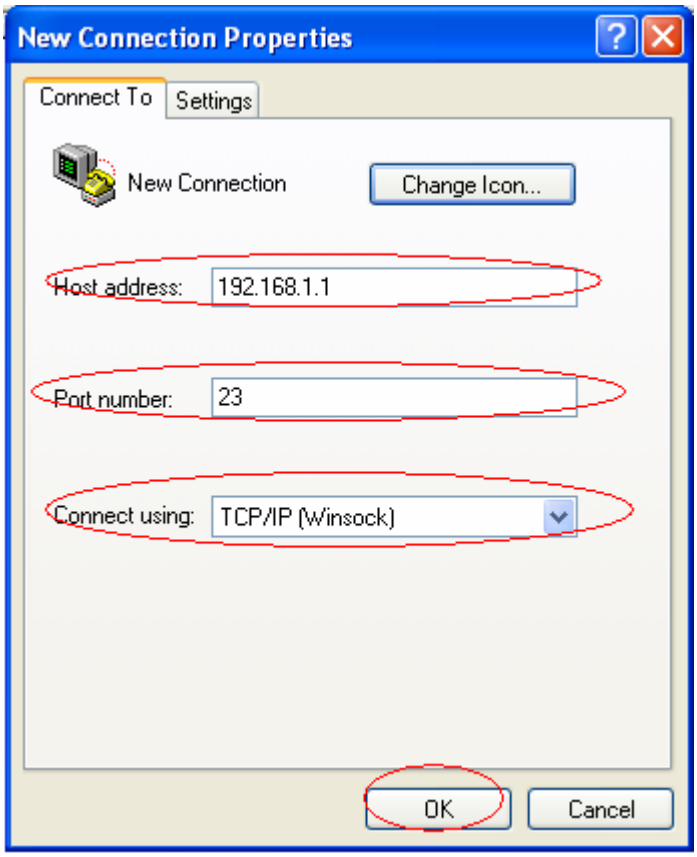
- **Capture the detailed logs by Hyper Terminal**

Step 1: Initiate a hyper terminal connection from your PC(suppose you connected to the LAN port of P-661H-D)

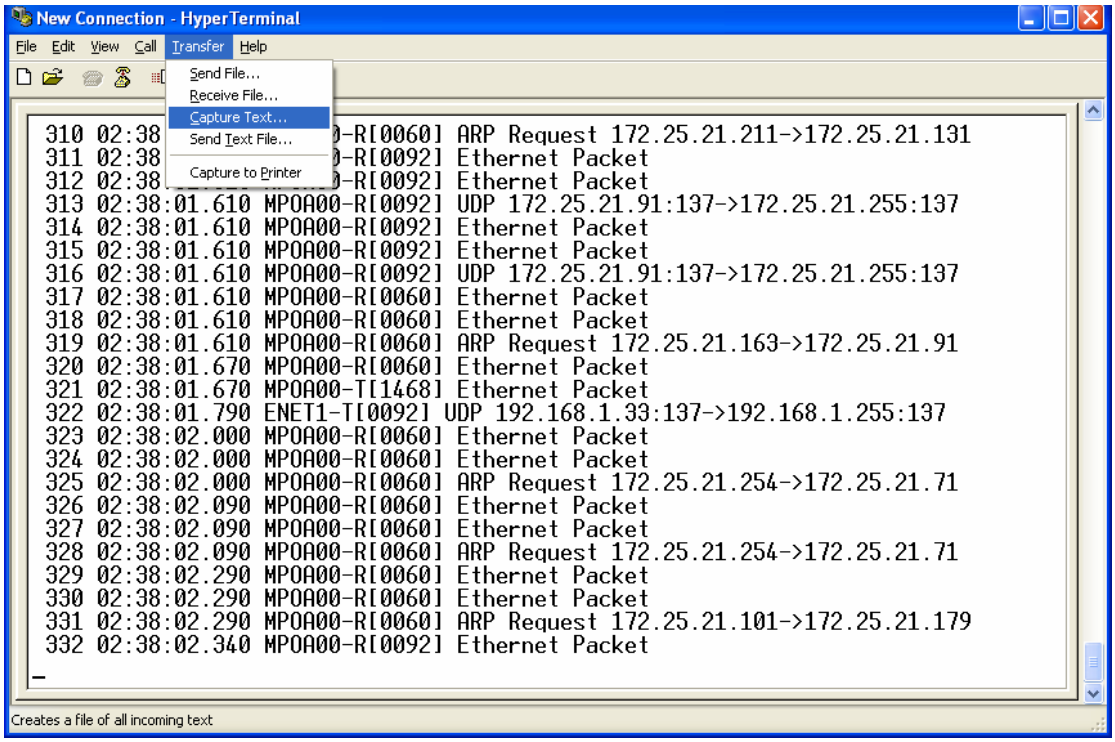



Step 2: Click the ‘properties’ to configure parameters to telnet to the P-661H-D.




Step 3: So that after you invoke the relevant commands, you could save the logs you've captured.




## 2. Firmware/Configurations Uploading and Downloading using TFTP

- **Using TFTP client software**

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

**(1) Using TFTP to upload/download ZyNOS via LAN**

Step 1: TELNET to your Prestige first before running the TFTP software

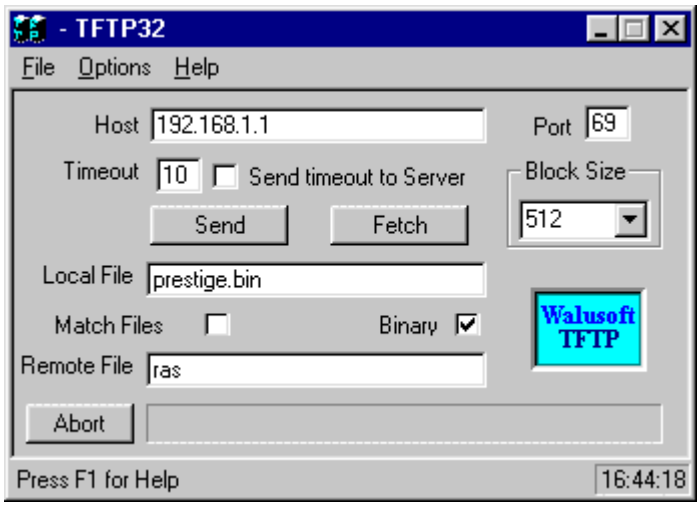
Step 2: Type the CI command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI)**

Step 3: Run the TFTP client software

Step 4: Enter the IP address of the Prestige

Step 5:To upload the firmware, please save the remote file as **'ras'** to Prestige. After the transfer is complete, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.

**An example:**




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.

**(2) Using TFTP to upload/download SMT configurations via LAN**

Step 1: TELNET to your Prestige first before running the TFTP software

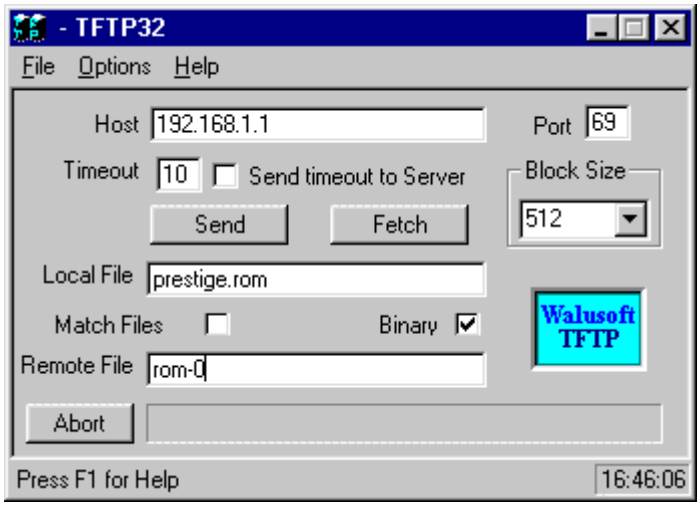
Step 2: Type the command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI).**

Step 3: Run the TFTP client software

Step 4: To download the P-661H-D configuration, please get the remote file **'rom-0'** from the Prestige.

Step 5: To upload the P-661H-D 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**

Step 1: TELNET to your Prestige first before using TFTP command
Step 2: Type the CI command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI).**
Step 3: Download ZyNOS via LAN : **c:\tftp -i [PrestigeIP] get ras [localfile]**
Step 4: Upload P-661H-D configurations via LAN: **c:\tftp -i [PrestigeIP] put [localfile] rom-0**
Step 5: Download P-661H-D configurations via LAN: **c:\tftp -i [PrestigeIP] get rom-0 [localfile]**

- **Using TFTP command on UNIX**

**Before you begin:**

1. TELNET to your Prestige first before using TFTP command
2. Type the CI command 'sys stdio 0' to disable console idle timeout in **Command Line Interface (CLI)**

Example:

```
[cppwu@faelinux cppwu]$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Password: ****
ras> sys stdio 0
(Open a new window)
[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 get rom-0 [local-rom] <- change to binary mode

<- download configurations

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

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

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

### 3. Using FTP to Upload the Firmware and Configuration Files

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

To use this feature, your workstation must have a FTP client software. See the example shown below.

- **Using FTP client software**

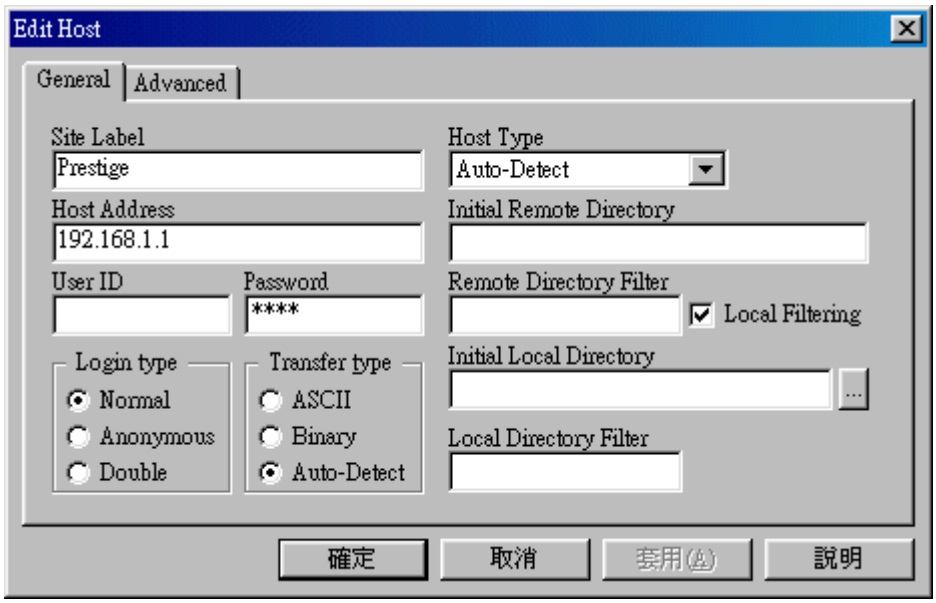
Note: The remote file name for the firmware is **'ras'** and the configuration file is **'rom-0'**.

| | |
|---|---|
| **Step 1** | Use FTP client from your workstation to connect to the Prestige by entering the IP address of the Prestige. |
| **Step2** | Press **'Enter'** key to ignore the username, because the Prestige does not check the username. |
| **Step 3** | Enter the **CLI** password as the FTP login password, the default is **'admin**'. |
| **Step 4** | Enter command **'bin'** to set the transfer type to binary. |
| **Step 5** | Use **'put'** command to transfer the file to the Prestige. |

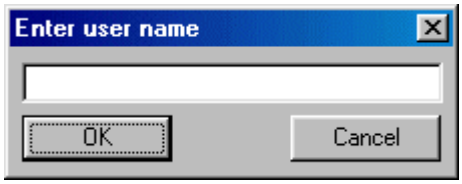
**Example:**

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

**'Binary'**.

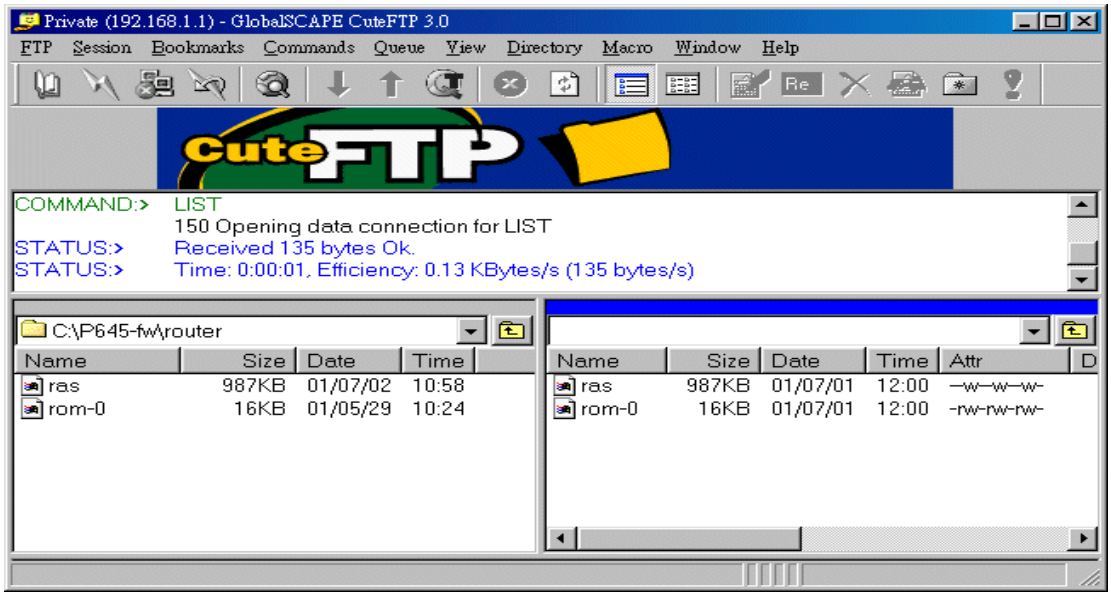



Step 2: Press **'OK'** to ignore the 'Username' prompt.




Step 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.



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

# CI Command Reference

Command Syntax and General User Interface

CI has the following command syntax:

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

General user interface:

| | | |
|---|---|---|
| **1.** | **?** | Shows the following commands and all major (sub)commands |
| **2.** | **exit** | Exit Subcommand |

**To get the latest CI Command list**

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