P-660HN-T1A

802.11n 1x1 Wireless ADSL2+ 4-port Gateway

Support Notes

Version3.40

Apr. 2010

ZyXEL
Unleash Networking Power

FAQ

System FAQ

1. What's Multilingual Embedded Web Configurator?

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

2. How do I access the P-660HN-T1A 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.

3. How do I update the firmware and configuration file?

You can do this if you access the P-660HN-T1A 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 firmware.

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

The P-660HN-T1A allows you to transfer the firmware to P-660HN-T1A using TFTP program via LAN. The procedure for uploading firmware via TFTP is as follows.

   a. Use the TELNET client program in your PC to login to your P-660HN-T1A.
   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-660HN-T1A 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.

5. How do I restore P-660HN-T1A configurations by using TFTP client program via LAN?

   a. Use the TELNET client program in your PC to login to your P-660HN-T1A.
   b. Enter CI command **'sys stdio 0'** disable Stdio idle timeout
   c. To backup the P-660HN-T1A configurations, use TFTP client program to get file **'rom-0'** from the P-660HN-T1A.
   d. To restore the P-660HN-T1A configurations, use the TFTP client program to put your configuration in file **rom-0** in the P-660HN-T1A.

6. 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-660HN-T1A 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'.**

7. How to use the Reset button?

   a. Turn your P-660HN-T1A 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.
   c. Press the **RESET** button for six seconds and then release it. If the **POWER** LED begins to blink, the default configuration has been restored and the P-660HN-T1A restarts.

8. 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

7

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.

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

There will be three options for you:

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

SUA (Single User Account) 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-660HN-T1A 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-660HN-T1A supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The P-660HN-T1A 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.**

10. 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-660HN-T1A 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**).

11. 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.

12. 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-660HN-T1A maps one ILA to one IGA.
- **Many to One:** In Many-to-One mode, the P-660HN-T1A maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA is optional in today's Prestige routers).
- **Many to Many Overload:** In Many-to-Many Overload mode, the P-660HN-T1A maps the multiple ILA to shared IGA.
- **Many One-to-One:** In Many One-to-One mode, the P-660HN-T1A maps each ILA to unique IGA.
- **Server:** In Server mode, the P-660HN-T1A 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 ILA2<--->IGA1 ...

Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many One-to-One	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

13. 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-660HN-T1A supports 4k 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.

14. What are Device filters and Protocol filters?

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**.

15. How can I protect against IP spoofing attacks?

The P-660HN-T1A'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-660HN-T1A?

- 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-660HN-T1A 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-660HN-T1A and check the current system status.

For Administrator Account, besides accessing the status monitor of P-660HN-T1A, it can also access Wizard setup/ Advanced setup of P-660HN-T1A:

Moreover, only with Administrator Password, you could manage the P-660HN-T1A via FTP/TFTP or Telnet.

4. How do I know the P-660HN-T1A'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-660HN-T1A 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-660HN-T1A 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-660HN-T1A to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660HN-T1A, 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-660HN-T1A.

When the ISP assigns the P-660HN-T1A a new IP, the P-660HN-T1A 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-660HN-T1A sends this IP to the DDNS server for its updates.

11. What is DDNS wildcard? Does the P-660HN-T1A 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-660HN-T1A 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. 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-660HN-T1A but only one VC activated at one time, the P-660HN-T1A 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.

13. Why do we perform traffic shaping in the P-660HN-T1A?

The P-660HN-T1A 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-660HN-T1A 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-660HN-T1A to avoid congestion; traffic shaping takes measures to adapt to unpredictable fluctuations in traffic flows and other problems among virtual connections.

14. 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-660HN-T1A 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.)

15. 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):

16. 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-660HN-T1A performs content filtering. You can also specify trusted IP Addresses on LAN for which the P-660HN-T1A will not perform content filtering. You can configure the details about it in Web Configurator, Advanced setup, **Security -> 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 24 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-660HN-T1A's front panel is on when the ADSL physical layer is up.

5. How does the P-660HN-T1A work on a noisy ADSL?

Depending on the line quality, the P-660HN-T1A 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:

```
relative capacity occupation: 100%
noise margin upstream: 6.0 db
output power downstream: 10.4 dbm
attenuation upstream: 1.2 db
carrier load: number of bits per symbol(tone)
tone   0- 31: 00 00 00 08 ab cd de ee ee ee fe ee ed dd cb b9
tone  32- 63: 04 44 56 67 88 9a ab bc cc dd dd de ee ee ee ee
tone  64- 95: ee ee ee ee ee ee ff ff ff ff ff ff ee ff ff fe
tone  96-127: fe ee ee ee ee ee ee ee ef ef ee fe ee ef fe ff
tone 128-159: fe ff fe fe ee ee ee fe ef ff ff ff fe fe ee ef
tone 160-191: ff ff ff ff ff fe ff ef ff ff ff ff ff ff ff ff
tone 192-223: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
tone 224-255: ff ef ef ee ef ff ee ef ee fe fe fe ff ff ff fe
relative capacity occupation: 100%
noise margin downstream: 12.4 db
```

[ATMStatus]   [ATM Loopback Test]   [DSL Line Status]   [Reset ADSL Line]
[Capture All Logs]

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

The signaling pins on the P-660HN-T1A'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 …
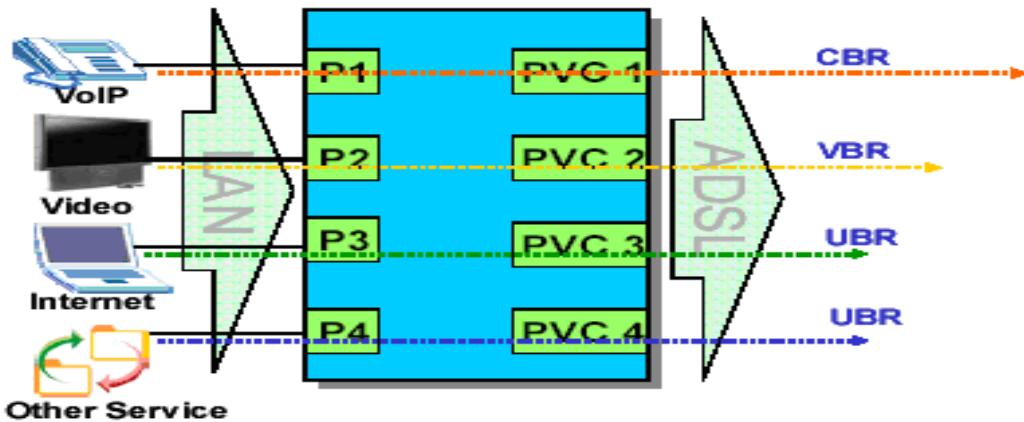
Triple Play is a port-based policy to forward packets from different LAN port to different PVCs, thus you can configure each PVC separately to assign different QoS to different application.

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-660HN-T1A secure?

The P-660HN-T1A 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-660HN-T1A 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 in the P-660HN-T1A?

1. The P-660HN-T1A'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-660HN-T1A'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-660HN-T1A'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-660HN-T1A'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-660HN-T1A'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-660HN-T1A?

There are two default ACLs pre-configured in the P-660HN-T1A, 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-660HN-T1A. By factory default, if you connect your PC to the LAN Interface of P-660HN-T1A, 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-660HN-T1A'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-660HN-T1A:

| WWW | Telnet | FTP | SNMP | DNS | ICMP |

WWW

Server Port   80
Server Access   LAN & WAN
Secured Client IP Address   ⦿ All   ○ Selected 0.0.0.0

Note :
1: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

Apply   Cancel
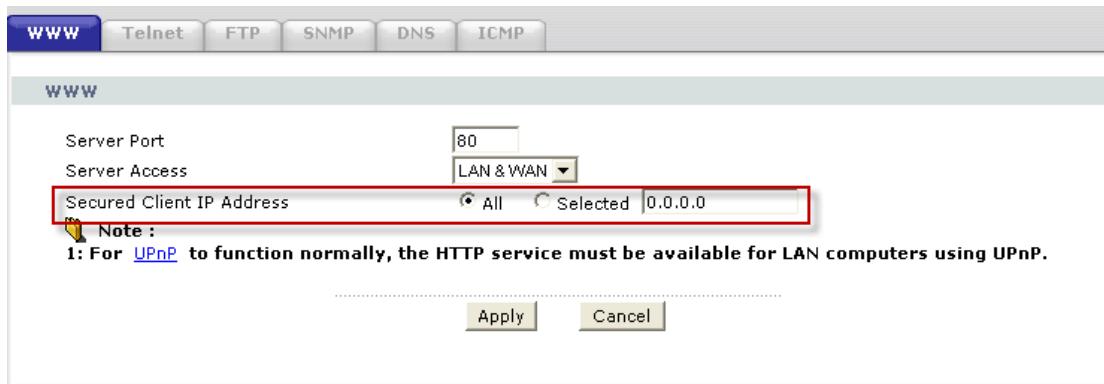
The default value in this field is 0.0.0.0, which means you do not care which host is trying to telnet your P-660HN-T1A or access.the Web Configurator of

3. Why can't I configure my P-660HN-T1A 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:**

WWW	Telnet	FTP	SNMP	DNS	ICMP

Telnet

Server Port	23
Server Access	LAN & WAN ▼
Secured Client IP Address	⦿ All ○ Selected 0.0.0.0

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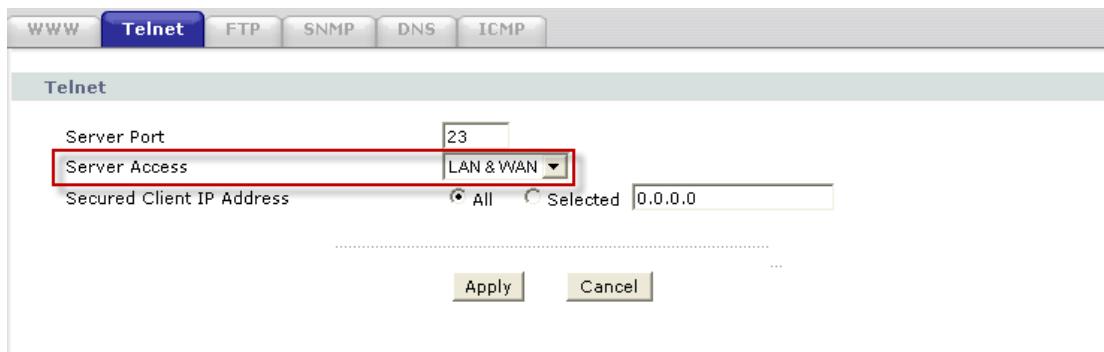
(3) WWW/Telnet service is enabled but your host IP is not the secured host entered in Web Configurator, Advanced setup, **Advanced -> Remote MGNT:**

WWW	Telnet	FTP	SNMP	DNS	ICMP

Telnet

Server Port	23
Server Access	LAN & WAN ▼
Secured Client IP Address	⦿ All ○ Selected 0.0.0.0

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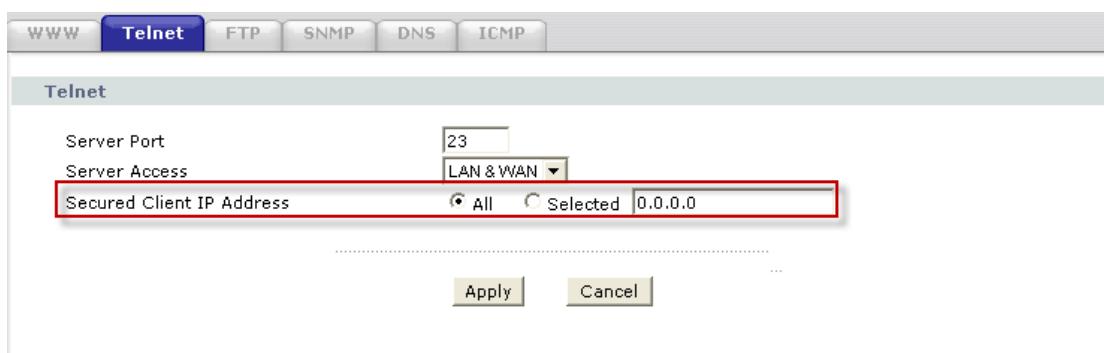
(4)A filter set which blocks WWW/Telnet from WAN is applied to WAN node. You can check by command:
wan node index [index #]
wan node display

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-660HN-T1A'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-660HN-T1A generate the firewall log?

The P-660HN-T1A 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-660HN-T1A, 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-660HN-T1A generate the firewall alert?

The P-660HN-T1A 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-660HN-T1A 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.

Wireless FAQ

General FAQ

1. What is a Wireless LAN?

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

2. What are the advantages of Wireless LAN?

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

Installation Speed and Simplicity: Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

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

Reduced Cost-of-Ownership: While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.

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

3. What is the disadvantage of Wireless LAN?

The speed of Wireless LAN is still relatively slower than wired LAN. The setup cost of Wireless LAN is relative high because the equipment cost including access point and PCMCIA Wireless LAN card is higher than hubs and CAT 5 cables.

4. Where can you find 802.11 wireless networks?

Airports, hotels, and even coffee shops like Starbucks are deploying 802.11 networks, so people can wirelessly surf the Internet with their laptops.

5. What is an Access Point?

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

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

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

7. What is Wi-Fi?

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

8. What types of devices use the 2.4GHz Band?

Various spread spectrum radio communication applications use the 2.4 GHz band. This includes WLAN systems (not necessarily of the type IEEE

802.11b), cordless phones, wireless medical telemetry equipment and Bluetooth™ short-range wireless applications, which include connecting printers to computers and connecting modems or hands-free kits to mobile phones.

9. Does the 802.11 interfere with Bluetooth device?

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

10. Can radio signals pass through wall?

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

11. What are potential factors that may causes interference among WLAN products?

Factors of interference:
(1) Obstacles: walls, ceilings, furniture… etc.
(2) Building Materials: metal door, aluminum studs.
(3) Electrical devices: microwaves, monitors, electric motors.
Solution:
(1) Minimizing the number of walls and ceilings
(2) Antenna is positioned for best reception
(3) Keep WLAN products away from electrical devices, eg: microwaves, monitors, electric motors,…, etc.
(4) Add additional APs if necessary.

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

WLANs are generally privately owned, wireless systems that are deployed in a corporation, warehouse, hospital, or educational campus setting. Data rates are high and there are no per-packet charges for data transmission.
WWANs are generally publicly shared data networks designed to provide coverage in metropolitan areas and along traffic corridors. WWANs are owned by a service provider or carrier. Data rates are low and charges are based on usage. Specialized applications are characteristically designed around short, burst messaging.

13. Can I manually swap the wireless module without damage any hardware?

Yes, it will not harm the hardware, but the module will not be detected and work after inserting to the slot. You need to reboot the router to initialize the module.

14. What wireless security mode does P-660HN-T1A support?

The wireless security modes supported on P-660HN-T1A are: Static WEP, WPA-PSK, WPA, WPA2-PSK, and WPAPSKMixed.

15. What Wireless standard does P-660HN-T1A support?

It supports IEEE 802.11b/g/draft n standard.

16. Does P-660HN-T1A support MAC filtering?

Yes, it supports up to 32 MAC Address filtering.

17. Does P-660HN-T1A support auto rate adaption?

Yes, it means that the AP on P-660HN-T1A will automatically decelerate when devices move beyond the optimal range, or other interference is present. If the device moves back within the range of a higher-speed transmission, the connection will automatically speed up again. Rate shifting is a physical-layer mechanism transparent to the user and the upper layers of the protocol stack.

Advanced FAQ

1. What is Ad Hoc mode?

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

2. What is Infrastructure mode?

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

3. How many Access Points are required in a given area?

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

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

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

5. What is Frequency-hopping Spread Spectrum Technology – (FHSS)?

FHSS uses a narrowband carrier which hops through a predefined sequence of several frequencies at a specific rate. This avoids problems with fixed channel narrowband noise and simple jamming. Both transmitter and receiver must have their hopping sequences synchronized to create the effect of a

single "logical channel". To an unsynchronised receiver an FHSS transmission appears to be short-duration impulse noise. 802.11 may use FHSS or DSSS.

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

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

7. Why the 2.4 GHZ Frequency range?

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

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

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

Security FAQ

1. How do I secure the data across the P-660HN-T1A Access Point's radio link?

To secure the date across the P-660HN-T1A Access Point's radio link, we could select any one of the security mode: **Static 64/128 bit WEP, WPA-PSK, WPA, WPA2-PSK, WPA2.**

2. What is WEP?

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

3. What is WPA-PSK?

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

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

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

5. What is a WEP key?

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

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

No. 128-bit WEP will not communicate with 64-bit WEP. Although 128 bit WEP also uses a 24 bit Initialization Vector, but it uses a 104 bit as secret key. Users need to use the same encryption level in order to make a connection.

7. Can the SSID be encrypted?

No, WEP only encrypts the data packets not the 802.11n management

packets.The SSID is in the beacon and probe management messages and SSID goes over the air in clear text. This makes obtaining the SSID easy by sniffing 802.11n wireless traffic.

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

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

9. What are Insertion Attacks?

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

10. What is Wireless Sniffer?

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

Application Notes

General Application Notes

1. Internet Access Using P-660HN-T1A under Bridge mode

- Setup your workstation
- Setup your P-660HN-T1A 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-660HN-T1A 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-660HN-T1A's LAN port, the computer must have an Ethernet adapter card installed. For connecting a single computer to the P-660HN-T1A, 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.
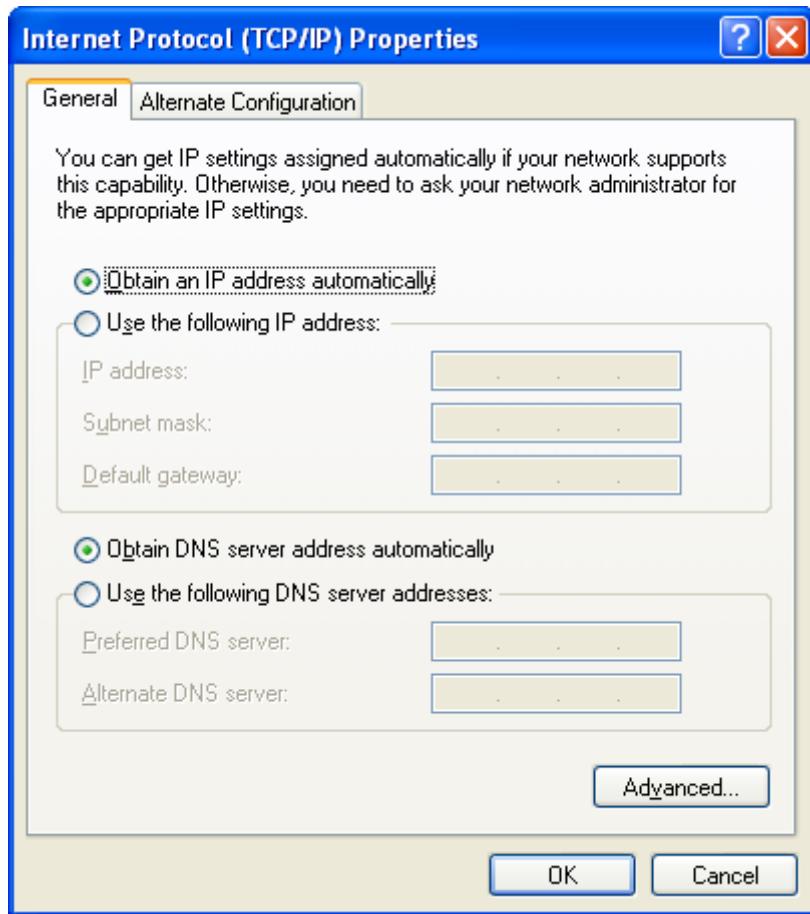
Setup your P-660HN-T1A under bridge mode

The following procedure shows you how to configure your P-660HN-T1A as bridge mode. We will use Web Configurator to guide you through the related menu.

1. Retrieve Prestige Web

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

2. Login first

The default username and password is the default SMT password **'1234'**.

(1) Configure P-660HN-T1A 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-660HN-T1A in Web Configurator, Advanced Setup, **Network -> LAN**. We use 192.168.1.1 as the LAN IP for P-660HN-T1A in this case:

Step 1: Disactive DHCP Server and apply it:

Step 2: Assign an IP to the LAN Interface of P-660HN-T1A, e.g.: 192.168.1.1:

2. Internet Access Using P-660HN-T1A 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-660HN-T1A 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-660HN-T1A using Ethernet cable.

(2) TCP/IP configuration

Since the P-660HN-T1A 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-660HN-T1A. The P-660HN-T1A 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.
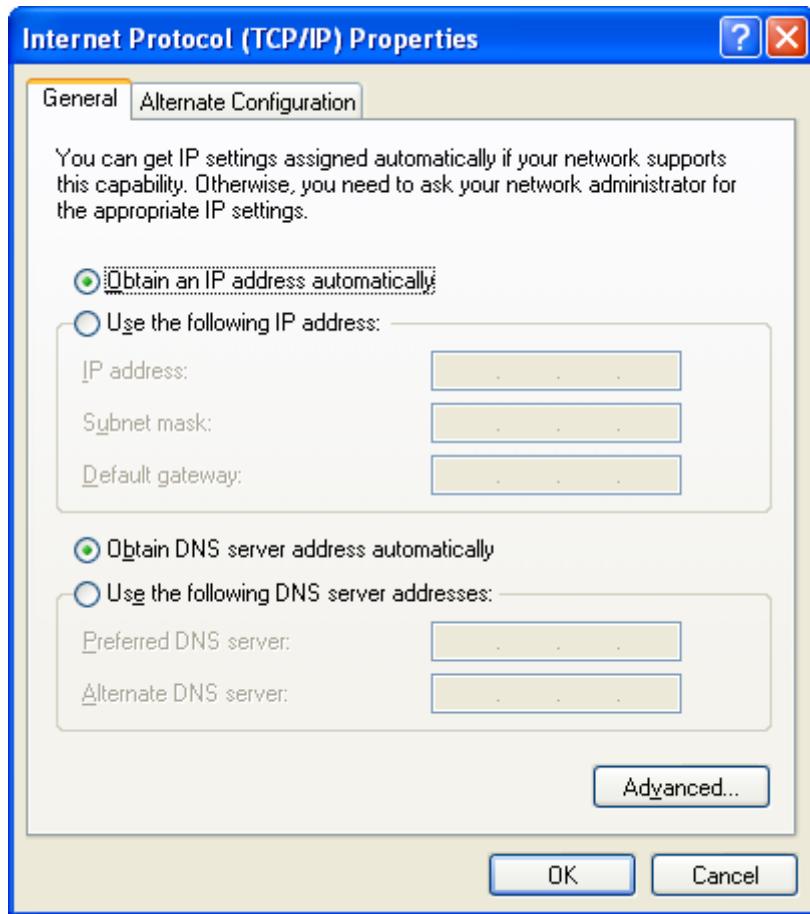
Set up your P-660HN-T1A under routing mode

The following procedure shows you how to configure your P-660HN-T1A as Routing mode for routing traffic. We will use Web Configurator to guide you through the related menu.

(1) Configure P-660HN-T1A 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-660HN-T1A dynamically. Otherwise, set to **Static** and enter the IP in the **IP Address** field.

(2) Configure a LAN IP for the P-660HN-T1A and the DHCP settings in Web Configurator, Advanced Setup, **Network -> LAN.**

3. Setup the P-660HN-T1A as a DHCP Relay

- **What is DHCP Relay?**

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P-660HN-T1A 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
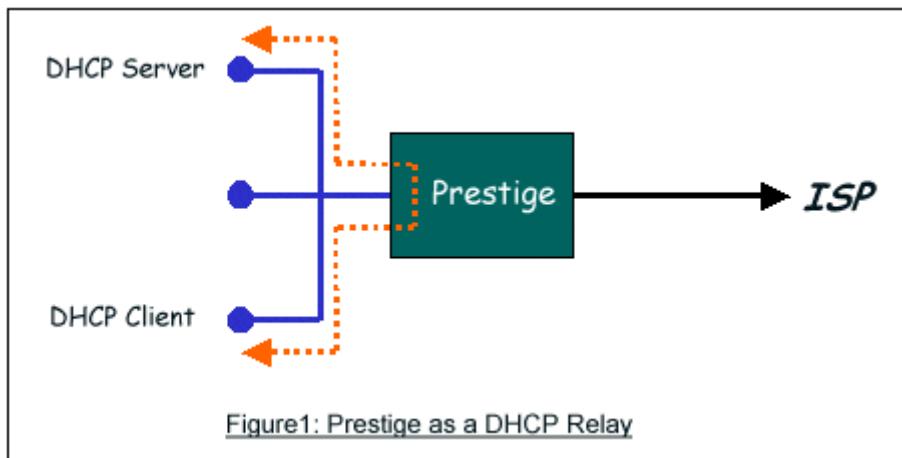
- **Setup the P-660HN-T1A as a DHCP Relay**

We could set the P-660HN-T1A as a DHCP Relay by the following command in **CLI**:
Ip dhcp enif0 mode relay

lp dhcp enif0 relay server [Server IP Address]

4. SUA Notes

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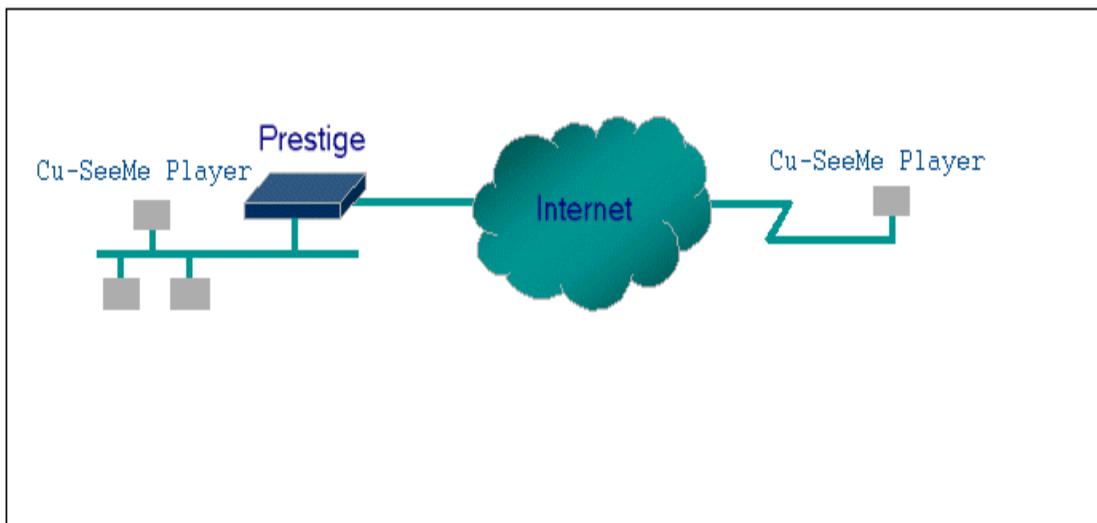
Introduction

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-660HN-T1A. 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-660HN-T1A'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. For DCC, please set Default/Client IP	.
Windows PPTP	None	1723/client IP
ICQ 99a	None for Chat. For DCC, please set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
ICQ 2000b	None for Chat	None for Chat
ICQ Phone 2000b	None	6701/client IP
Cornell 1.1 Cu-SeeMe	None	7648/client IP
White Pine 3.1.2 Cu-SeeMe[2]	7648/client IP & 24032/client IP	Default/client IP
White Pine 4.0 Cu-SeeMe	7648/client IP & 24032/client IP	Default/client IP
Microsoft NetMeeting 2.1 & 3.01[3]	None	1720/client IP 1503/client IP
Cisco IP/TV 2.0.0	None	.
RealPlayer G2	None	.
VDOLive	None	.
Quake1.06[4]	None	Default/client IP
QuakeII2.30[5]	None	Default/client IP
QuakeIII1.05 beta	None	.
StartCraft.	6112/client IP	.
Quick Time 4.0	None	.
pcAnywhere 8.0	None	5631/client IP 5632/client IP 22/client IP
IPsec (ESP tunneling mode)	None (one client only)	Default/Client
Microsoft Messenger Service 3.0	6901/client IP	6901/client IP
Microsoft Messenger Service 4.6/ 4.7/ 5.0/··· (none UPnP)[6]	None for Chat, File transfer ,Video and Voice	None for Chat, File transfer, Video and Voice

Net2Phone	None	6701/client IP
Network Time Protocol (NTP)	None	123 /server IP
Win2k Terminal Server	None	3389/server IP
Remote Anything	None	3996 - 4000/client IP
Virtual Network Computing (VNC)	None	5500/client IP 5800/client IP 5900/client IP
AIM (AOL Instant Messenger)	None for Chat and IM	None for Chat and IM
e-Donkey	None	4661 - 4662/client IP
POLYCOM Video Conferencing	None	Default/client IP
iVISTA 4.1	None	80/server IP
Microsoft Xbox Live[7]	None	N/A

[1] Since SUA enables your LAN to appear as a single computer to the Internet, it is not possible to configure similar servers on the same LAN behind SUA.

[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-660HN-T1A 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-660HN-T1A 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-660HN-T1A is an alternative solution to pass through MSN Messenger video/ voice traffic. For more detail, please refer to UPnP application note.

[7] P-660HN-T1A 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-660HN-T1A's *WAN IP* address which can be obtained from Web Configurator, **Status -> WAN Information**.

Configure an Internal Server behind SUA
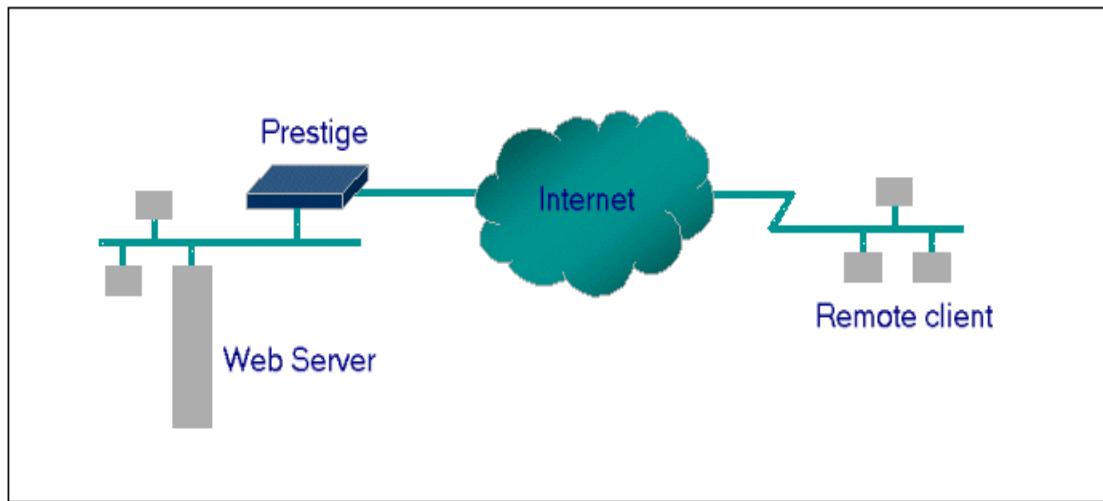
Introduction

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-660HN-T1A, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time P-660HN-T1A 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-660HN-T1A'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.
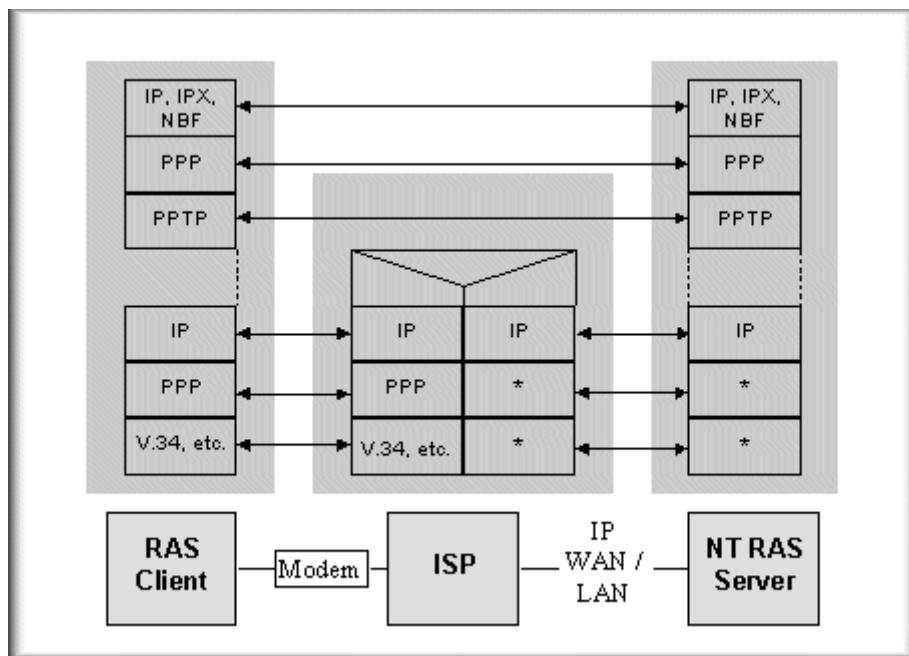
Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

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-660HN-T1A SUA case. 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-660HN-T1A to forward to the appropriate private IP address of Windows NT server.
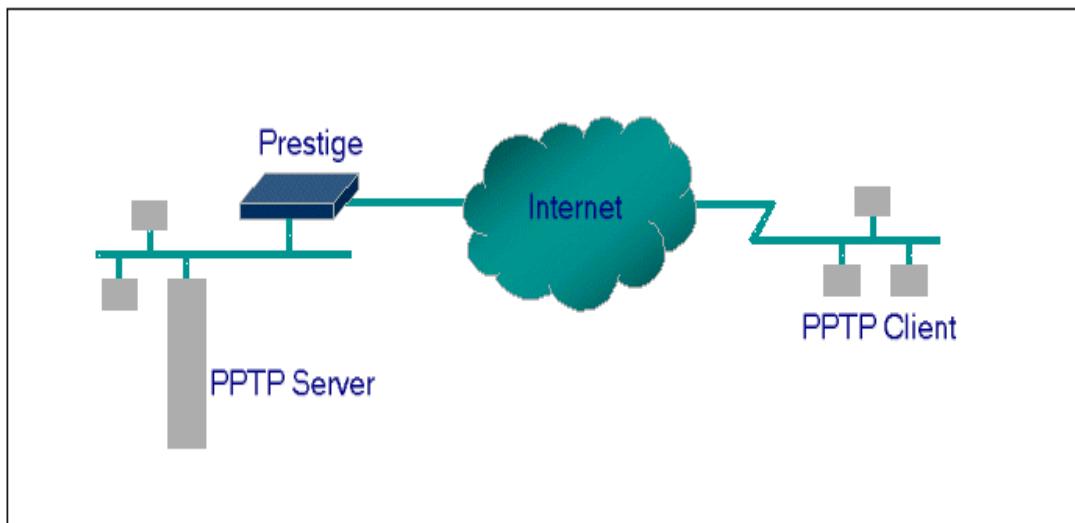
Example

The following example shows how to dial to an ISP via the P-660HN-T1A 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-660HN-T1A.

(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-660HN-T1A

(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-660HN-T1A's Internet IP address for logging to NT RAS server.
- Set the Internet gateway to the router that is connecting to ISP

(3) P-660HN-T1A setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect P-660HN-T1A 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'.

General	Port Forwarding	ALG

Default Server Setup

Default Server   192.168.1.34

Port Forwarding

Service Name PPTP ▼   Server IP Address 192.168.1.10   Add

#	Active	Service Name	Start Port	End Port	Port Translation Start Port End Port	Server IP Address	Modify

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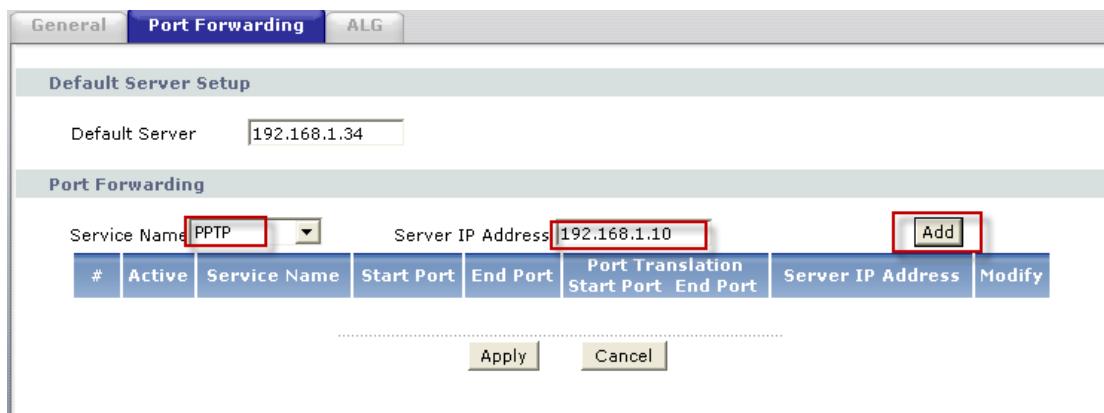
When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the Internet. If the Internet connection between two LANs is achievable, you can place a VPN call from the remote Win9x client.

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-660HN-T1A 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-660HN-T1A is in Routing mode, you can select NAT Option as Full Feature in Network -> NAT -> General:
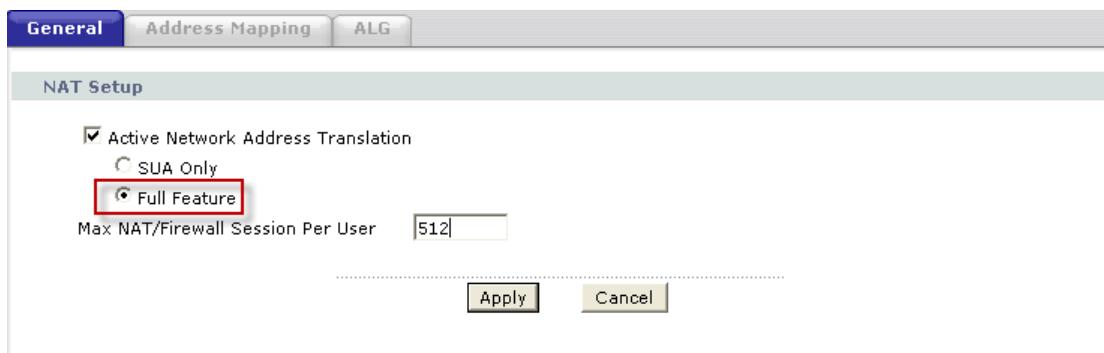
Key Settings:

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.
	SUA Only	When you select this option, this remote node will use default SUA Address Mapping Set.

Configuring NAT

Address Mapping Sets and NAT Server Sets

The P-660HN-T1A 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-660HN-T1A 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:**

General	**Address Mapping**	ALG				

Address Mapping Rules

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	-	-	-	-	-	✏ 🗑
2	-	-	-	-	-	✏ 🗑
3	-	-	-	-	-	✏ 🗑
4	-	-	-	-	-	✏ 🗑
5	-	-	-	-	-	✏ 🗑
6	-	-	-	-	-	✏ 🗑
7	-	-	-	-	-	✏ 🗑
8	-	-	-	-	-	✏ 🗑
9	-	-	-	-	-	✏ 🗑
10	-	-	-	-	-	✏ 🗑

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 2. Many-to-One 3. Many-to-Many Overload 4. Many-to-Many No Overload 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-660HN-T1A. (We suppose the LAN IP Address of P-660HN-T1A 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
ras>
```

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 Example: > 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". Type is 0 - 4 = one-to-one, many-to-one, many-to-many-overload, many-to-many-non overload, inside-server Example: > 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

57
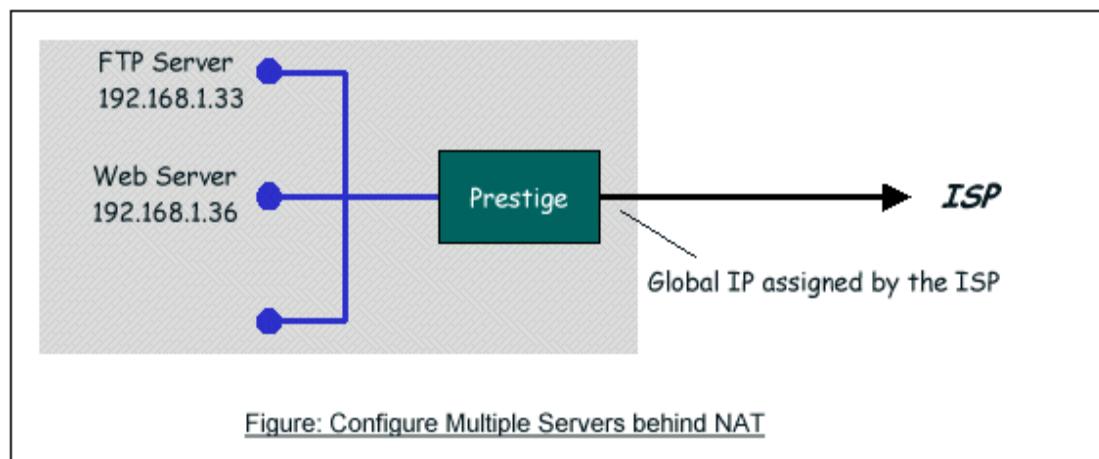
Please note that a server can support more than one service, e.g., a server can provide both FTP and Mail service, while another provides only Web service.

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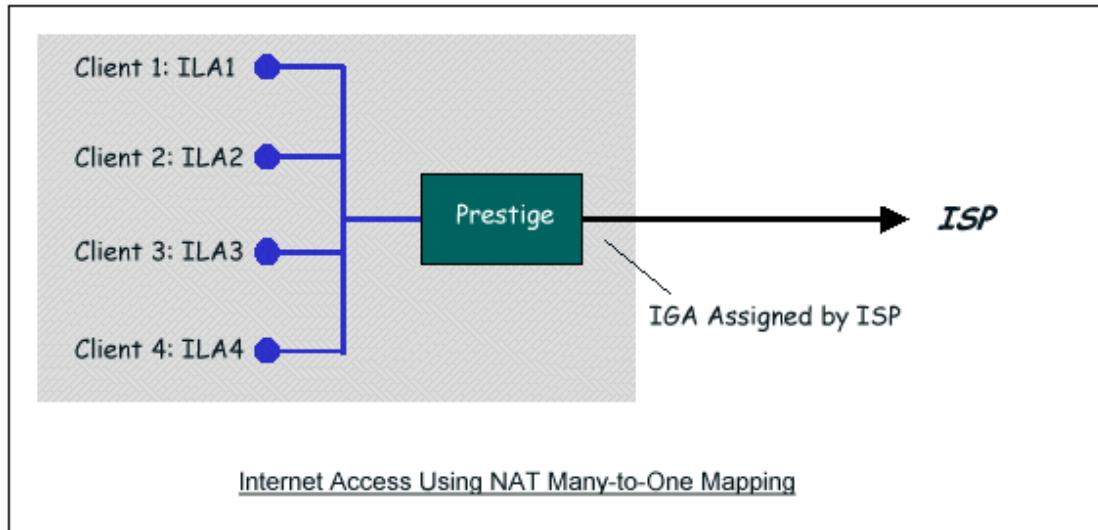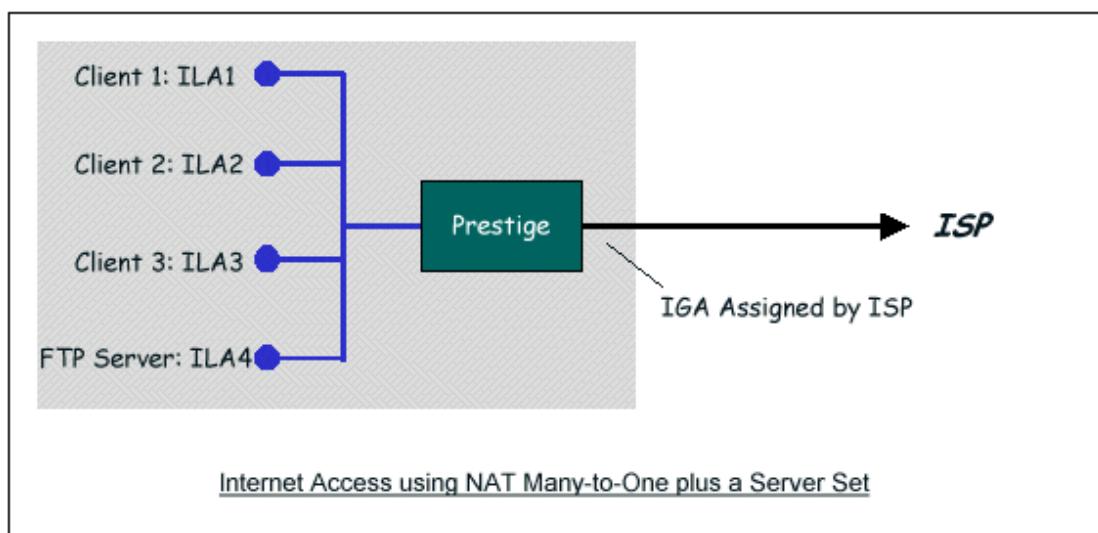
In this case, we do exactly as the figure (use the convenient pre-configured SUA Only set) and also go to Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** to specify the Internet Server behind the NAT as

below:

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

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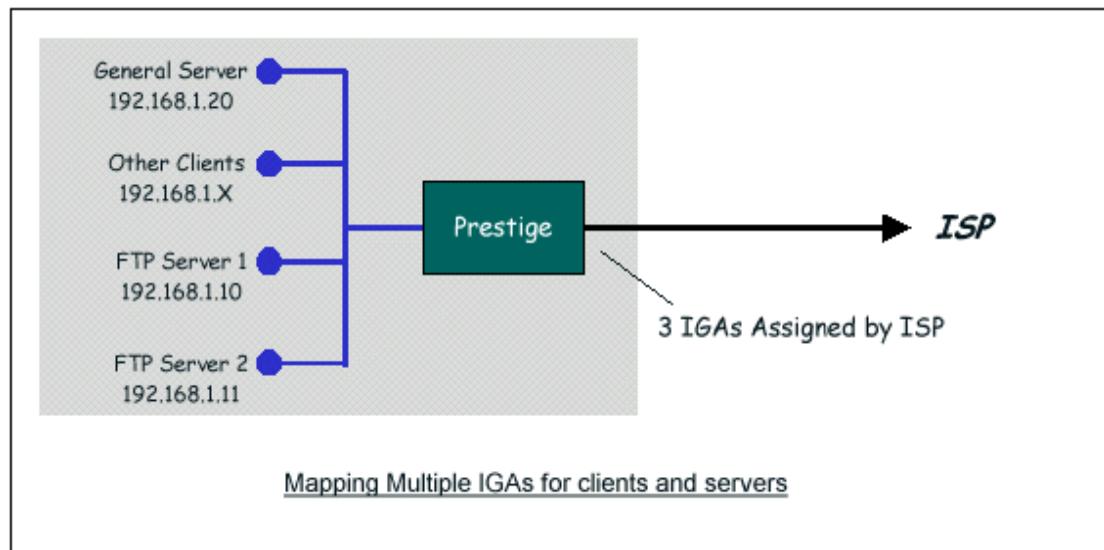
In this case we have 3 IGAs from the ISP. We have two very busy internal FTP servers and also an internal general server for the web and mail. In this case, we want to assign the 3 IGAs by the following way using 4 NAT rules.

- 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-660HN-T1A's WAN IP Address.

IP Address

○ Obtain an IP Address Automatically
⊙ Static IP Address
    IP Address   200.0.0.3
    Subnet Mask   255.255.255.0
    Gateway IP address   200.0.0.254

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).

Edit Address Mapping Rule1

Type   One-to-One
Local Start IP   192.168.1.10
Local End IP   N/A

Global Start IP   200.0.0.1
Global End IP   N/A
Server Mapping Set   PVC0 Edit Details

Back   Apply   Cancel

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).

Edit Address Mapping Rule2

Type	One-to-One
Local Start IP	192.168.1.11
Local End IP	N/A
Global Start IP	200.0.0.2
Global End IP	N/A
Server Mapping Set	PVC0 Edit Details

Back   Apply   Cancel

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

Edit Address Mapping Rule3

Type	Many-to-One
Local Start IP	0.0.0.0
Local End IP	255.255.255.255
Global Start IP	200.0.0.3
Global End IP	N/A
Server Mapping Set	PVC0 Edit Details

Back   Apply   Cancel

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

Edit Address Mapping Rule4

Type	Server
Local Start IP	N/A
Local End IP	N/A
Global Start IP	200.0.0.3
Global End IP	N/A
Server Mapping Set	PVC0 Edit Details

Back   Apply   Cancel

Menu **Network -> NAT -> Address Mapping** should look as follows now:
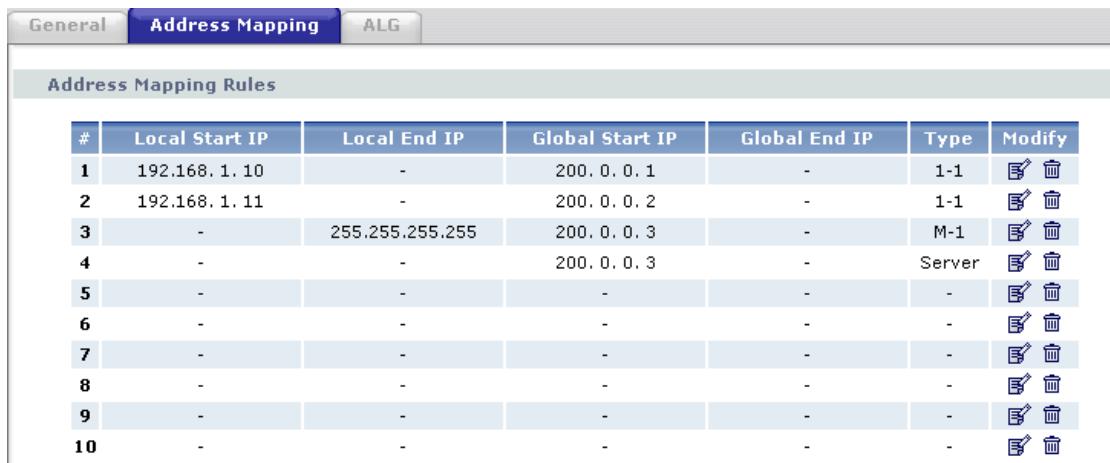
62

General	Address Mapping	ALG

Address Mapping Rules

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168.1.10	-	200.0.0.1	-	1-1	📝 🗑
2	192.168.1.11	-	200.0.0.2	-	1-1	📝 🗑
3	-	255.255.255.255	200.0.0.3	-	M-1	📝 🗑
4	-	-	200.0.0.3	-	Server	📝 🗑
5	-	-	-	-	-	📝 🗑
6	-	-	-	-	-	📝 🗑
7	-	-	-	-	-	📝 🗑
8	-	-	-	-	-	📝 🗑
9	-	-	-	-	-	📝 🗑
10	-	-	-	-	-	📝 🗑

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:**

General	Port Forwarding	ALG

Default Server Setup

Default Server   `10.10.1.2`

Port Forwarding

Service Name `WWW` ▼   Server IP Address `0.0.0.0`   [Add]

#	Active	Service Name	Start Port	End Port	Port Translation Start Port	End Port	Server IP Address	Modify
1	☑	WWW	80	80	80	80	192.168.1.20	📝 🗑
2	☑	FTP	20	21	20	21	192.168.1.20	📝 🗑

[Apply] [Cancel]

(4) Support Non NAT Friendly Applications

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

3 ILAs map to 3 IGAs using Many-to-Many No Overload or One-to-One type
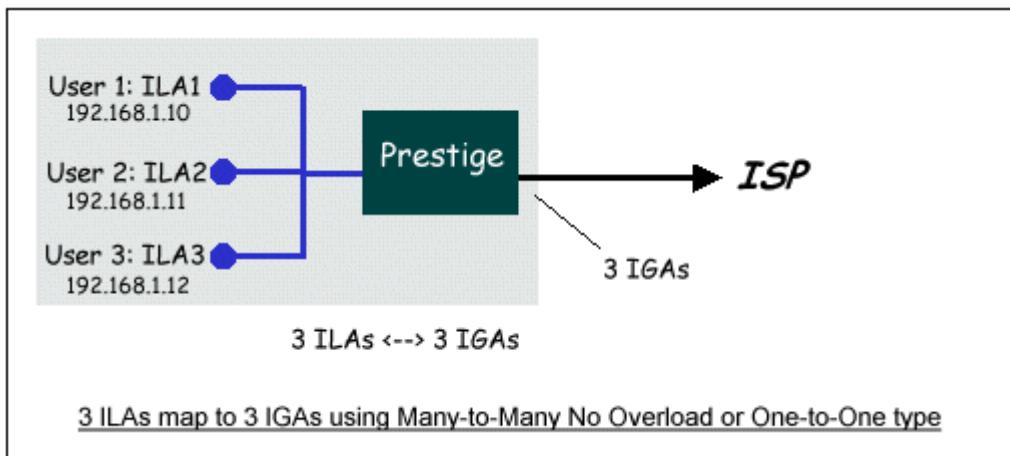
One rule configured for using **Many-to-Many No Overload** mapping type is shown below.

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-660HN-T1A to access the internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660HN-T1A, 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-660HN-T1A.

When the ISP assigns the P-660HN-T1A a new IP, the P-660HN-T1A 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-660HN-T1A 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-660HN-T1A, 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. **QoS(802.1Q)**

The QoS General Screen

Click Advanced > QoS to open the screen as shown next.Use this screen to enable or disable QoS, and select to have the ZyXEL Device automatically assign priority to traffic according to the IEEE 802.1p priority level, IP precedence and/or packet length.

General

Quality of Service	
QoS	○ Activated ⦿ Deactivated
Summary	QoS Settings Summary
Rule	
Rule Index	1 ▾
Active	○ Activated ⦿ Deactivated
Application	▾
Physical Ports	☐ ☐ ☐ ☐ ☐ WLAN Enet1 Enet2 Enet3 Enet4
Destination MAC	
IP	
Mask	
Port Range	~
Source MAC	
IP	
Mask	
Port Range	~
Protocol ID	▾
Vlan ID Range	~
IPP/DS Field	○ IPP/TOS ⦿ DSCP
IP Precedence Range	▾ ~ ▾
Type of Service	▾
DSCP Range	~ (Value Range: 0 ~ 63)
802.1p	▾ ~ ▾

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network. IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

8. Network Management Using SNMP

- ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some P-660HN-T1A 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
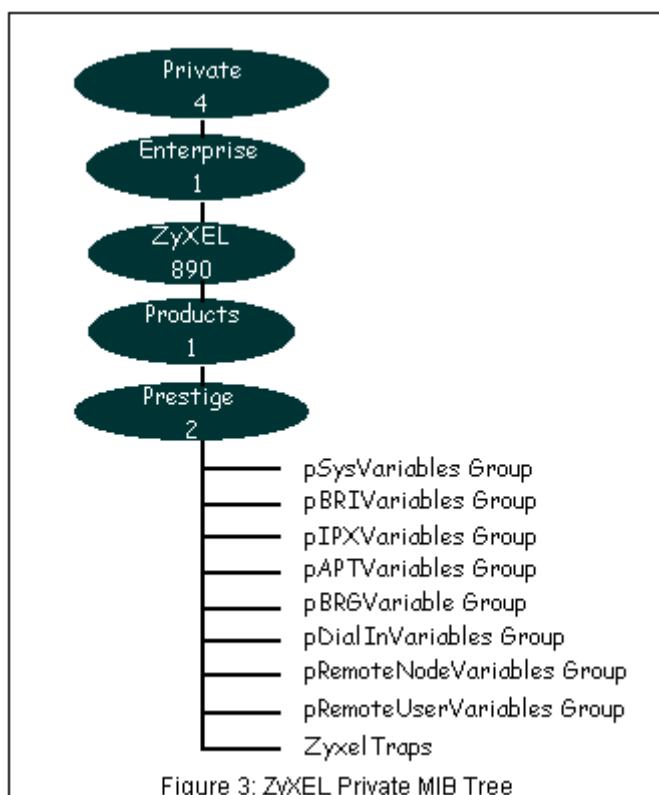
- *Downloading ZyXEL's private MIB*

- Configure the P-660HN-T1A for SNMP
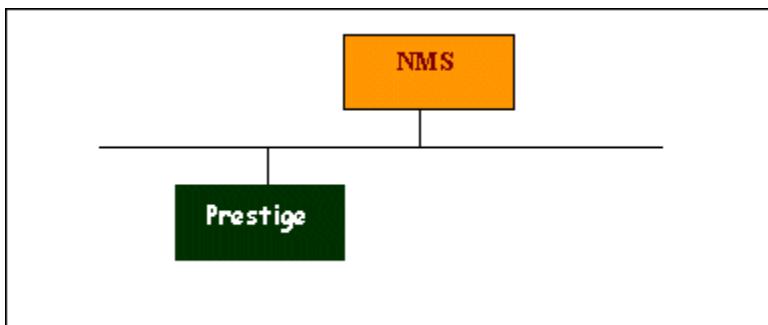
The SNMP related settings in P-660HN-T1A are configured in Web Configurator, Advanced Setup, **Advanced -> Remote MGNT -> SNMP** The following steps describe a simple setup procedure for configuring all SNMP settings.
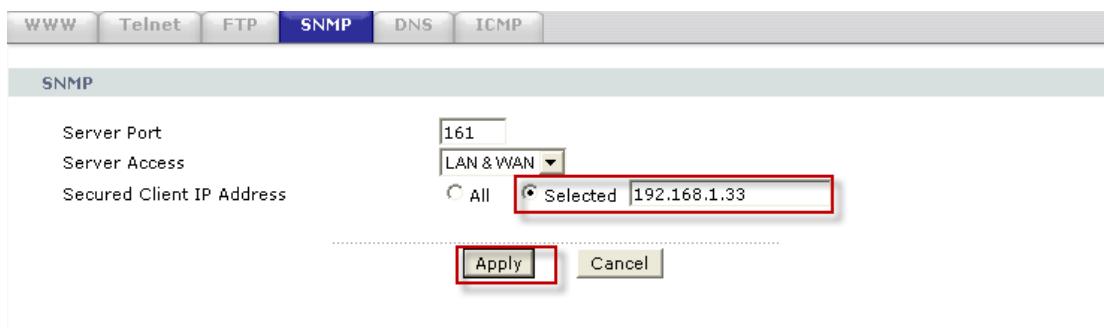
Note: You may need to edit a firewall rule to permit SNMP Packets.

9. Using syslog

All contents copyright © 2010 ZyXEL Communications Corporation.

You can configure it in Web Configurator, Advanced Setup, **Maintenance -> Logs -> System Log.**
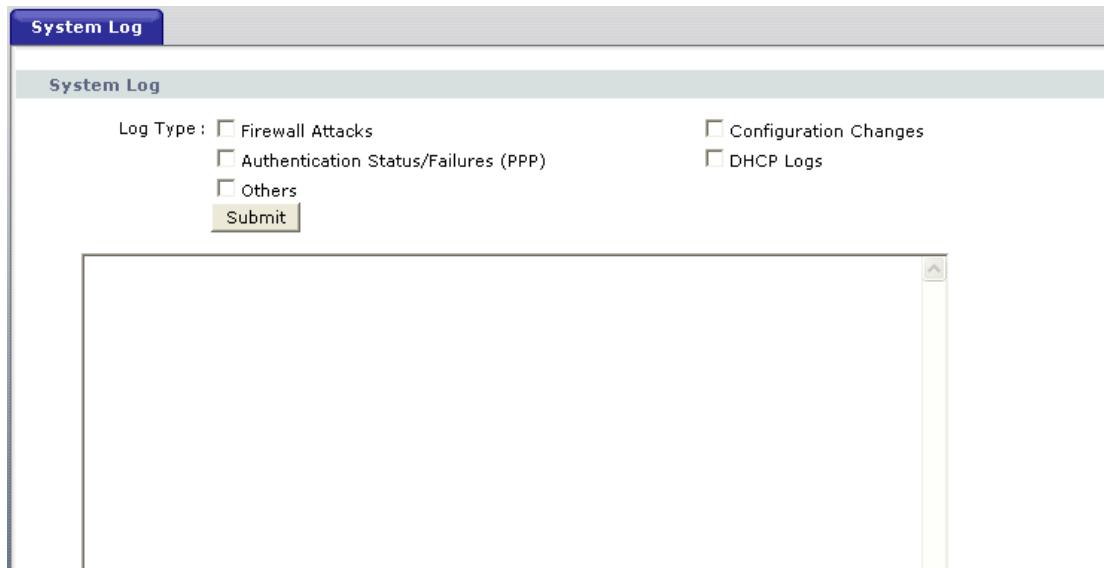
10. Using IP Alias

- **What is IP Alias ?**

In a typical environment, a LAN router is required to connect two local networks. The P-660HN-T1A 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-660HN-T1A's single user account. See the figure below.

The Prestige's IP Alias connects three local networks to the Internet
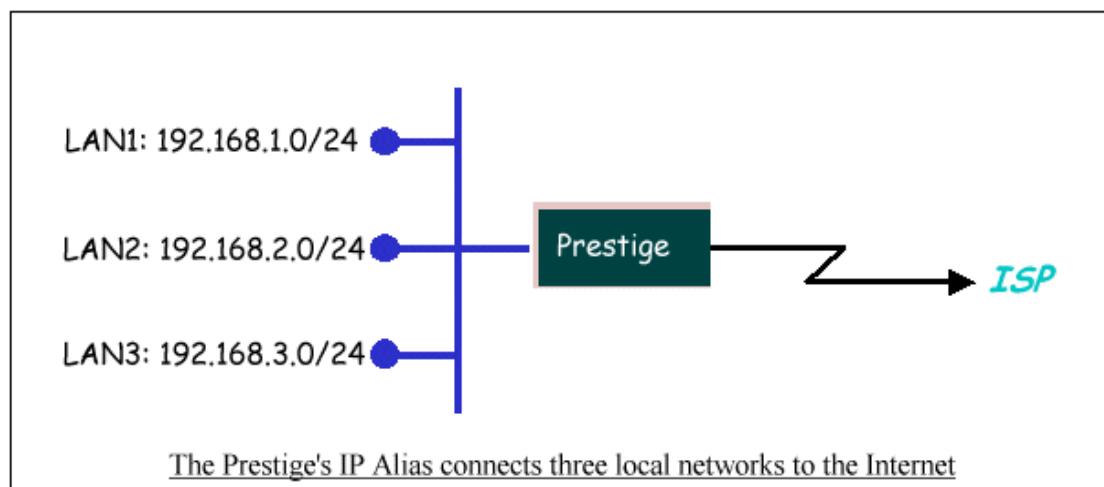
The P-660HN-T1A supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured in Web Configurator, Advanced Setup, **Network -> LAN -> DHCP Setup**. The second and third

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-660HN-T1A 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-660HN-T1A as shown below when the three networks are configured. If the P-660HN-T1A'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-660HN-T1A 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-660HN-T1A's first LAN IP address.

Key Settings:

DHCP Setup	If the P-660HN-T1A'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-660HN-T1A. 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-660HN-T1A's second and third LAN IP addresses.
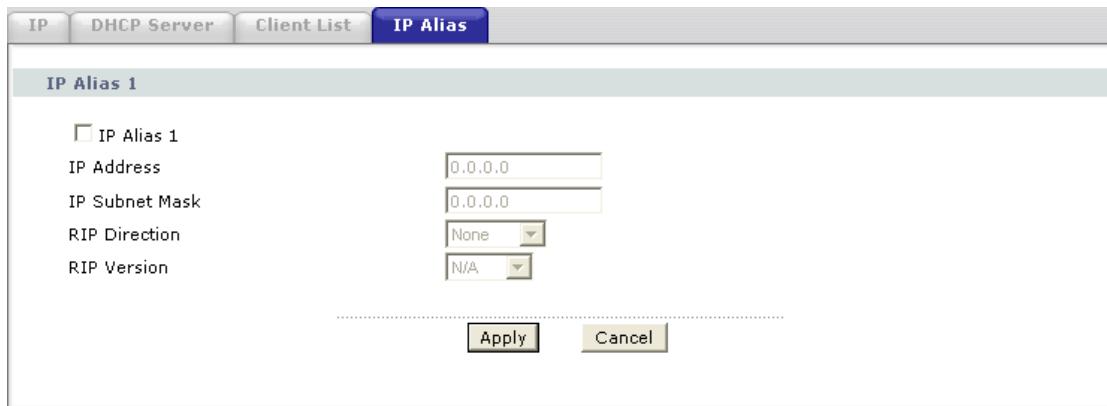

Key Settings:

IP Alias 1	Active it and enter the second LAN IP address for the P-660HN-T1A. This will create the second route in the enif0:0 interface.

11. 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.
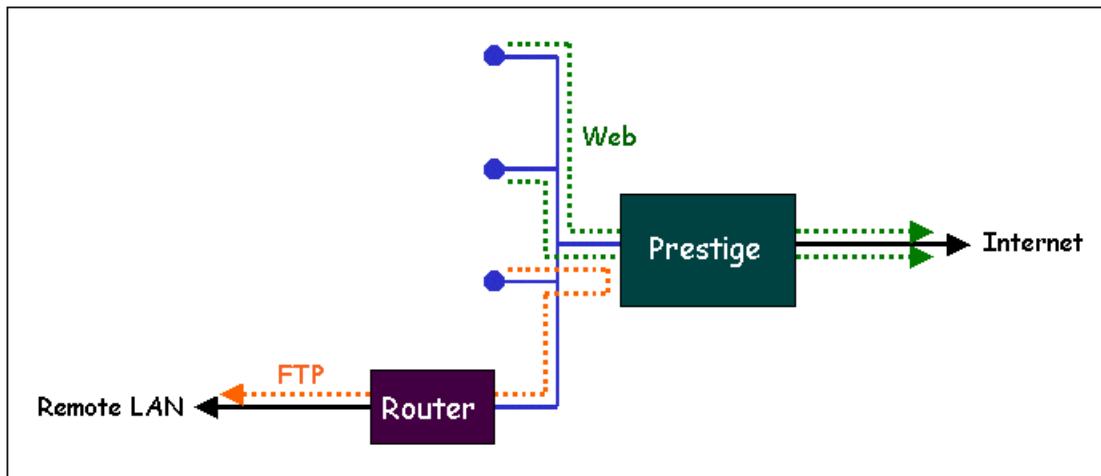
Use IPPR to distribute traffic among multiple paths

- 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 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

12. Using Call Scheduling

- What is Call Scheduling?

Call scheduling enables the mechanism for the P-660HN-T1A 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-660HN-T1A

There is no RTC (Real-Time Clock) chip so the P-660HN-T1A 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-660HN-T1A 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.**

Genreal	Time and Date

Current Time and Date

| Current Time | 01:55:00 |
| Current Date | 2000-01-01 |

Time and Date Setup

○ Manual
    New Time (hh:mm:ss)   1 : 54 : 29
    New Date (yyyy/mm/dd)   2000 / 1 / 1

● Get from Time Server
    Time Server Address   202.132.154.1

Time Zone Setup

Time Zone   (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London ▼
☐ Daylight Savings
Start Date   Last ▼ Sunday ▼ of January ▼ (2000-01-29) at 0 o'clock
End Date   Last ▼ Sunday ▼ of January ▼ (2000-01-29) at 0 o'clock

13. 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-660HN-T1A queries all directly connected networks to gather group membership.

After that, the P-660HN-T1A updates the information by periodic queries. The P-660HN-T1A implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

P-660HN-T1A supports IGMP v1 ,v2 and IGMP v3 without source filtering.

- **IP Multicast Setup**

(1) Enable IGMP in P-660HN-T1A's LAN in Web Configurator, Advanced Setup, **Network -> LAN -> IP -> Advanced Setup.**
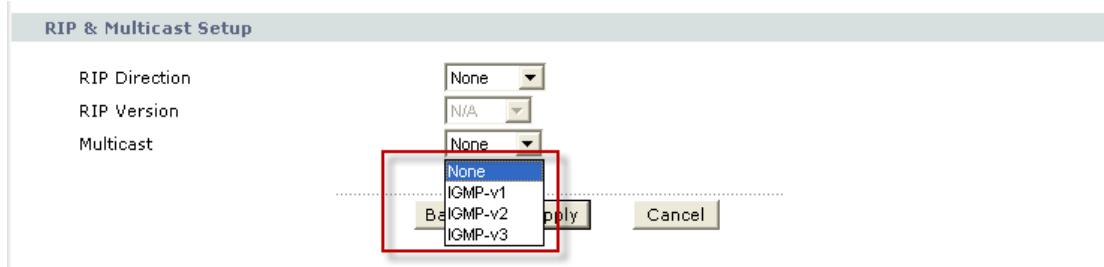
(2) Enable IGMP in P-660HN-T1A's remote node in Web Configurator, Advanced Setup, **Network -> WAN ->Internet Connection -> Advanced Setup.**
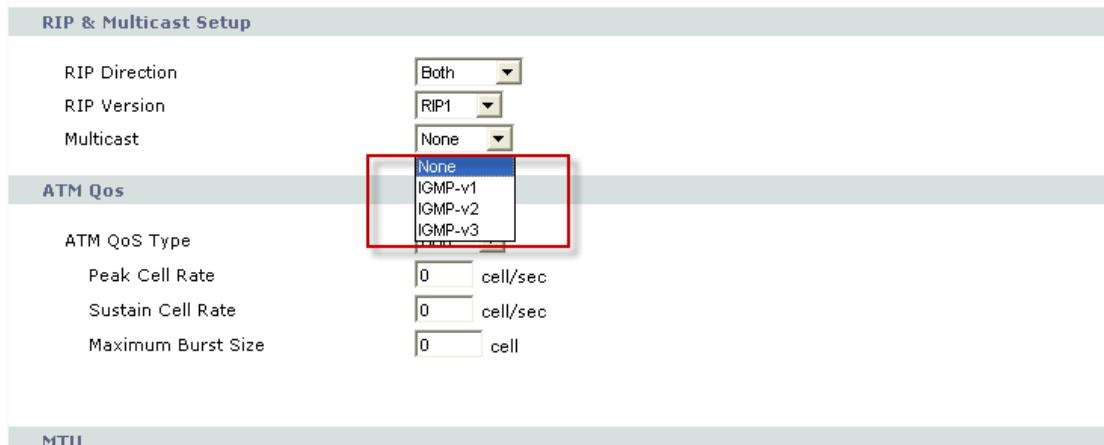
Key Settings:

Multicast	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2. IGMP-v3 for IGMP version 3

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|
```

15. How to configure packet filter on P-660HN-T1A?

The P-660HN-T1A 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-660HN-T1A 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:

```
Telnet 192.168.1.1
ras> sys filter set index 2 1
ras> sys filter set display
Set: 2 Rule: 1
Filter Type: TCP/IP
IP Protocol: 6
IP Source Route: No
Destination:
    IP Address: 0.0.0.0
    IP Mask: 0.0.0.0
    Port: 137
    Port Compare<0:None|1:Equal|2:NotEqual|3:Less|4:Greater>: 1
Source:
    IP Address: 0.0.0.0
    IP Mask: 0.0.0.0
    Port: 0
    Port Compare<0:None|1:Equal|2:NotEqual|3:Less|4:Greater>: 0
TCP Establish: No
Active: Yes
More: No
Log: None
Action Matched<1:Check Next|2:Forward|3:Drop>: 3
Action Not Matched<1:Check Next|2:Forward|3:Drop>: 1
ras>
```

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

16. Change WAN MTU via WEB-GUI.

You can change WAN MTU by: Network > WAN > Internet Connection > Advanced Setup, the default value is 1500.

Network > WAN > Advanced Setup

RIP & Multicast Setup

RIP Direction   None

RIP Version   N/A

Multicast   None

ATM Qos

ATM QoS Type   UBR

    Peak Cell Rate   0   cell/sec

    Sustain Cell Rate   0   cell/sec

    Maximum Burst Size   0   cell

MTU

MTU   1500

85
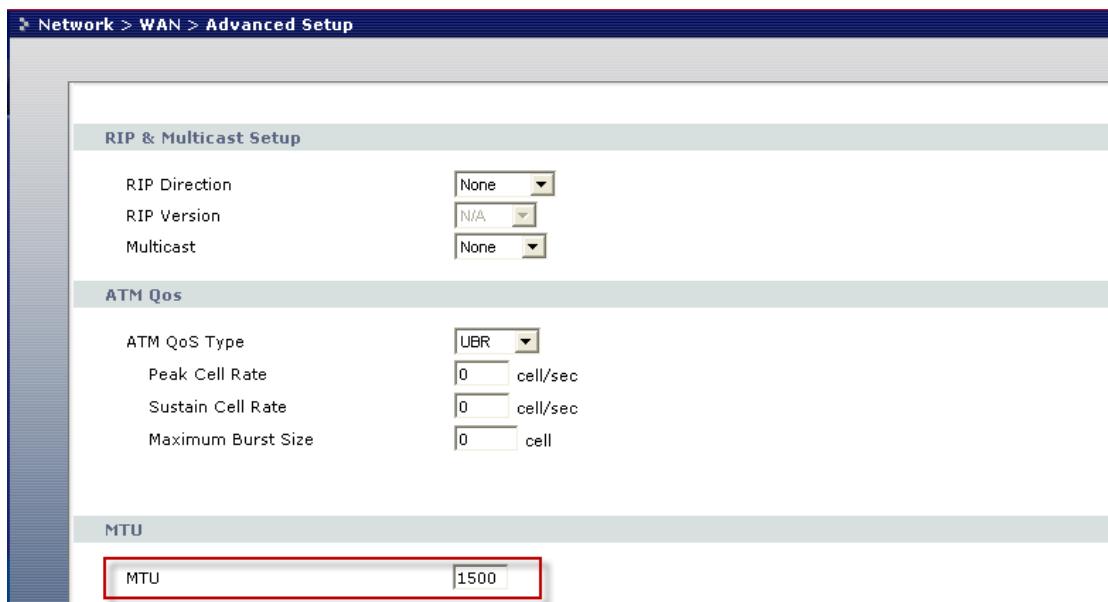
Wireless Application Notes

1. Configure a Wireless Client to Ad hoc mode

Ad hoc Introduction

What is Ad Hoc mode?
Ad hoc mode is a wireless network consists of a number of stations without access points. Without using an access point or any connection to a wired network, a client unit in Ad hoc operation mode can communicate directly to other client units just as using a cross over Ethernet cable connecting 2 host together via a NIC card for direct connection when configured in Ad hoc mode without an access point being present. Ad hoc operation is ideal for small networks of no more than 2-4 computers. Larger networks would require the use of one, or perhaps several, access points.
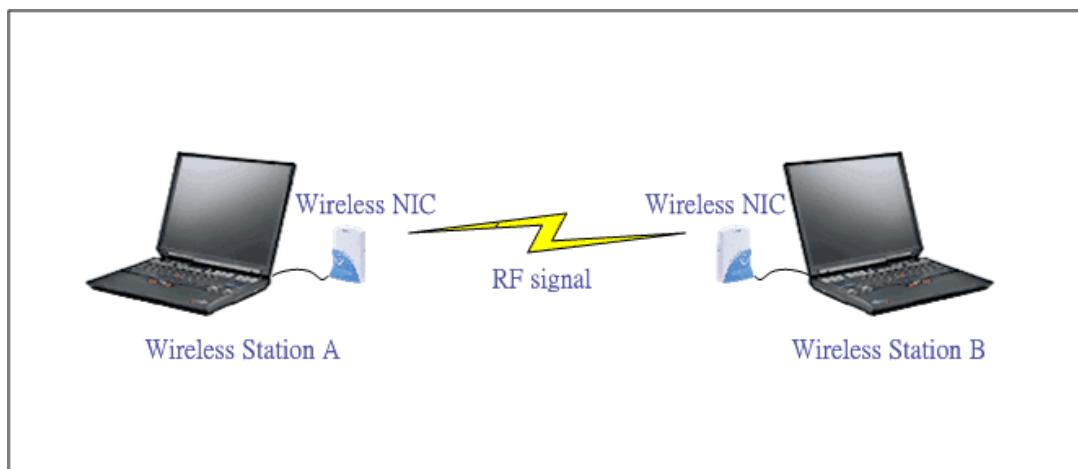
Configuration for Wireless Station A

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

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

Step 2: Select configuration tab.

Step 3: Select Ad hoc from the operation mode pull down menu, fill you an SSID and select a channel you want to use than press OK to apply.

Step 4: Since there is no DHCP server to give the host IP you must first designate a static IP for your station.   From Windows Start select Control Panel >Network Connection>Wireless Network Connection.

Step 5: From general tab select TCP/IP and click property
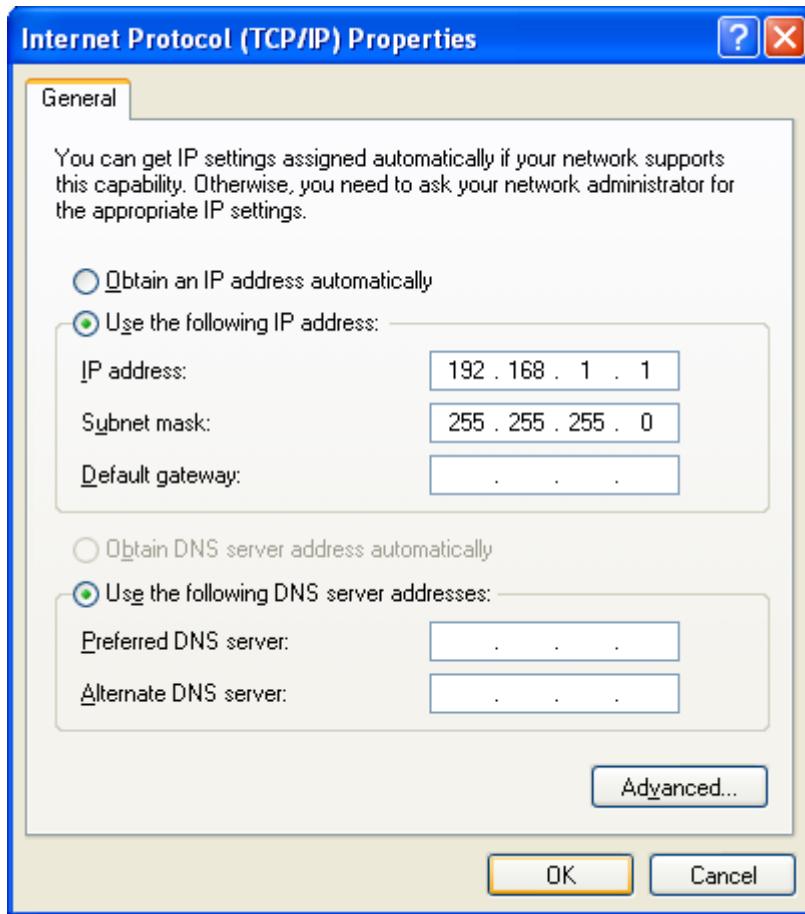
Step 6: Fill in your network IP address and subnet mask and click OK to finish.

Configuration for Wireless Station B

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

Step1: Double click on the utility icon in your windows task bar the utility will pop up on your windows screen.

Step 2: Select configuration tab.

Step 3: Select Ad hoc from the operation mode pull down menu, fill you an SSID and select a channel you want to use than press OK to apply.

Step 4: Since there is no DHCP server to give the host IP you must first designate a static IP for your station. From Windows Start select Control Panel >Network Connection>Wireless Network Connection.

Step 5: From general tab select TCP/IP and click property
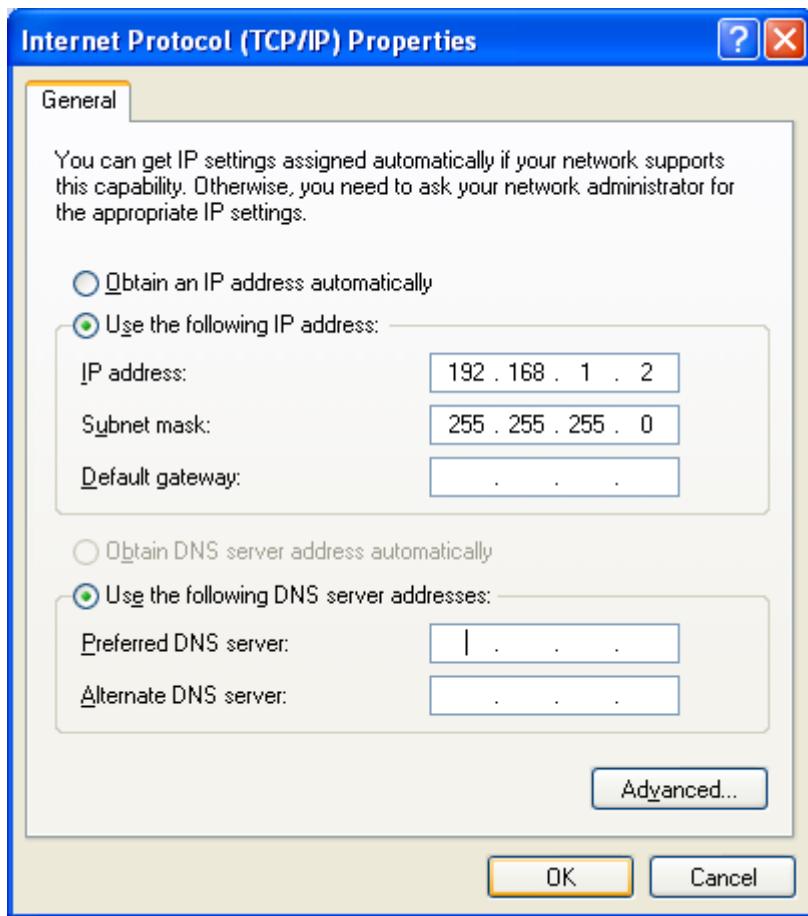
Step 6: Fill in your network IP address and subnet mask and click OK to finish.

Step 7: Station A now are able to connect to Station B.

2. MAC Filter

MAC Filter Overview

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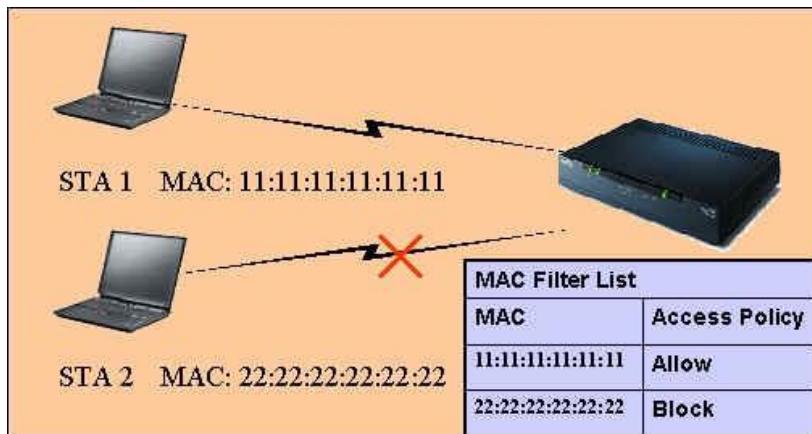
ZyXEL MAC Filter Implementation

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

Configure the WLAN MAC Filter

The MAC Filter related settings in ZyXEL APs are configured in Web Configurator, Advanced Setup, **Network -> Wireless LAN ->MAC Filter**. Before you configure the MAC filter, you need to know the MAC address of the client first. If not knowing what your MAC address is, please enter a command "**ipconfig /all**" after DOS prompt to get the MAC (physical) address of your wireless client.

Step 1: Login Web Configurator, Advanced Setup, **Network -> Wireless LAN ->MAC Filter**, active MAC Filter.

Step 2: Enter the MAC Addresses of wireless cards in the filter set to allow or deny association from these cards.

Key Settings:

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

	hosts with MAC addresses configured in this list will be blocked.
MAC Address	This field specifies those MAC Addresses that you want to add in the list.

3. Setup WEP (Wired Equivalent Privacy)

Introduction

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

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

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

Setting up the Access Point

You can set up the Access Point from Web configurator，**Network -> Wireless LAN -> AP.** (You can also configure it via **CLI**):

Step 1: Select '**Static WEP**' from the pull down menu 'Security Mode' in Web Configurator:

Step 2: Set up WEP Key in the Web Configurator. You need to set the one of the following parameters:

- o   64-bit WEP key (secret key) with 5 characters
- o   64-bit WEP key (secret key) with 10 hexadecimal digits
- o   128-bit WEP key (secret key) with 13 characters
- o   128-bit WEP key (secret key) with 26 hexadecimal digits
- o   256-bit WEP key (secret key) with 29 characters
- o   256-bit WEP key (secret key) with 58 hexadecimal digits

There are two ways you can configure the WEP Key.

(1) You can put in a special WEP key in the '**WEP Key**' menu directly.

(2) You can also put in an arbitrary sequence of characters in the '**Passphrase**' and then press button '**Generate**' to let the P-660HN-T1A generate WEP Key for you:
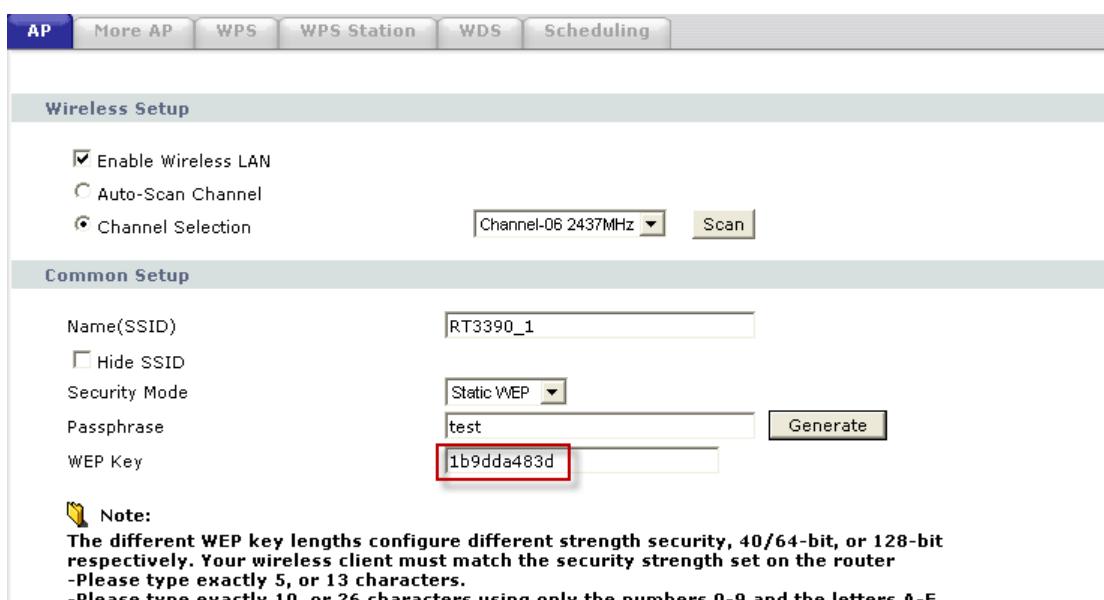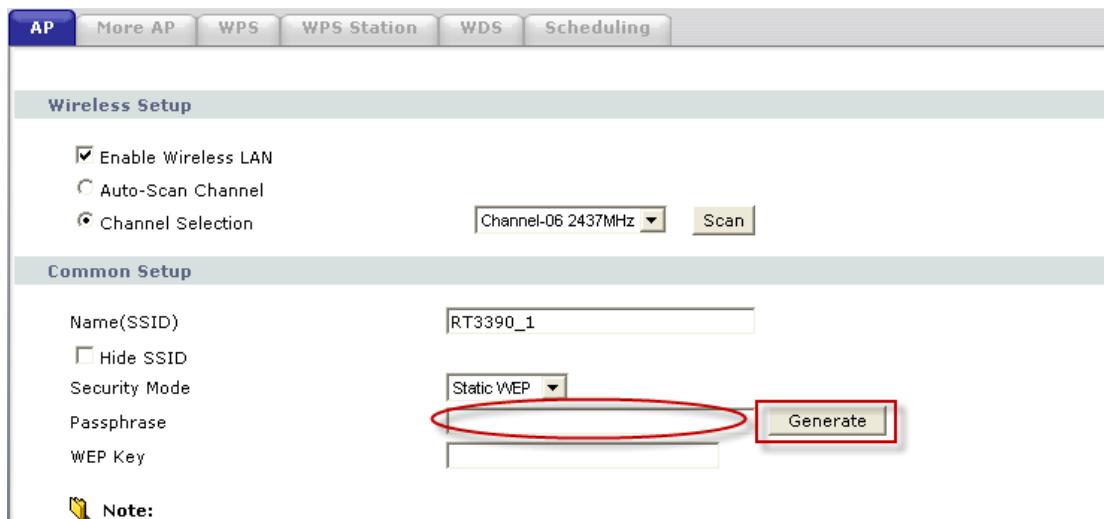
- **Setting up the Station**

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

The utility will pop up on your windows screen:
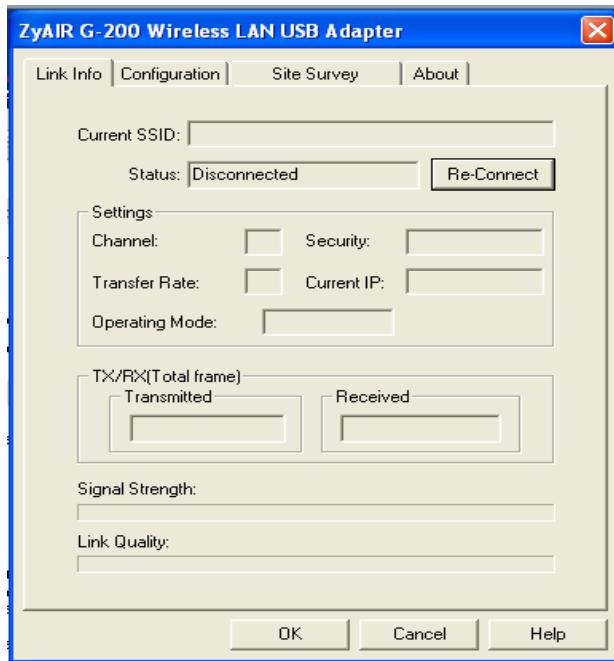
Note: If the utility icon doesn't exist in your task bar, click Start -> Programs -> ⋯⋯ to start the utility.

Step 2: Select the 'Configuration' tab.

Select 'Set Security' to configure encryption type and parameters correspond with access point.
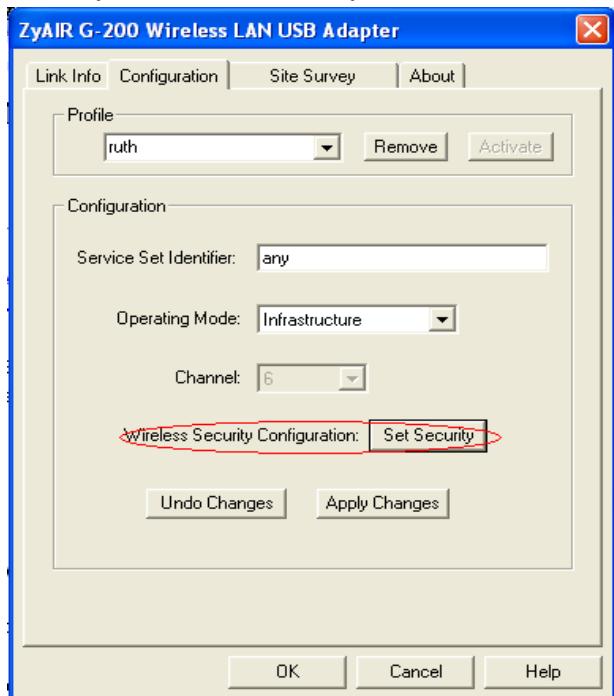
Note: You should select Key **1** as default Transmit Key, since the
P-660HN-T1A is supposed to use Key 1 by default.

Key settings

The WEP Encryption type of station has to equal to the access point.
Check 'ASCII' field for characters WEP key or **uncheck 'ASCII'** field for
Hexadecimal digits WEP key.
Hexadecimal digits don't need to preceded by '0x'.
For example:
64-bits with characters WEP key : Key1= 2e3f4
64-bits with hexadecimal digits WEP key : Key1= 123456789A

4. Site Survey

Introduction

What is Site Survey?

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

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

Preparation

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

1. First you will need to obtain a facility diagram, such as blueprints.   This is for you to mark and take record on.

2. Visually inspect the facility, walk through the facility to verify the accuracy of the diagram and mark down any large obstacle you see that may effect the RF signal such as metal shelf, metal desk, etc on the diagram.

3. Identify user's area, when doing so ask a question where is wireless coverage needed and where does not, and note and take note on the diagram this is information is needed to determine the number of AP required.

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

Survey on Site

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

Step 2: Install an access point at the preliminary location.

Step 3: Use a notebook with wireless client installed and run it's utility. An utility will provide information such as connection speed, current used channel, associated rate, link quality, signal strength and etc information as shown in utility below.
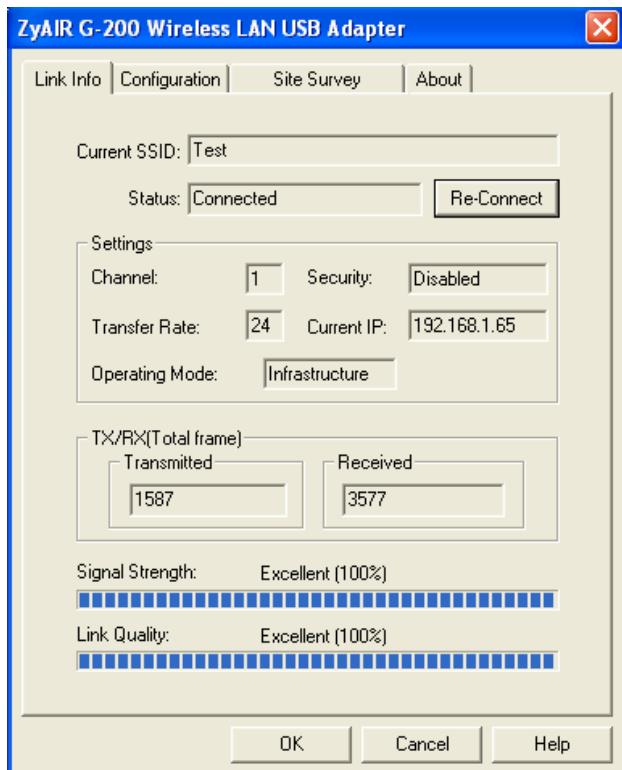
Step 4: It's always a good idea to start with putting the access point at the corner of the room and walk away from the access point in a systematic manner. Record down the changes at point where transfer rate drop and the link quality and signal strength information on the diagram as you go alone.
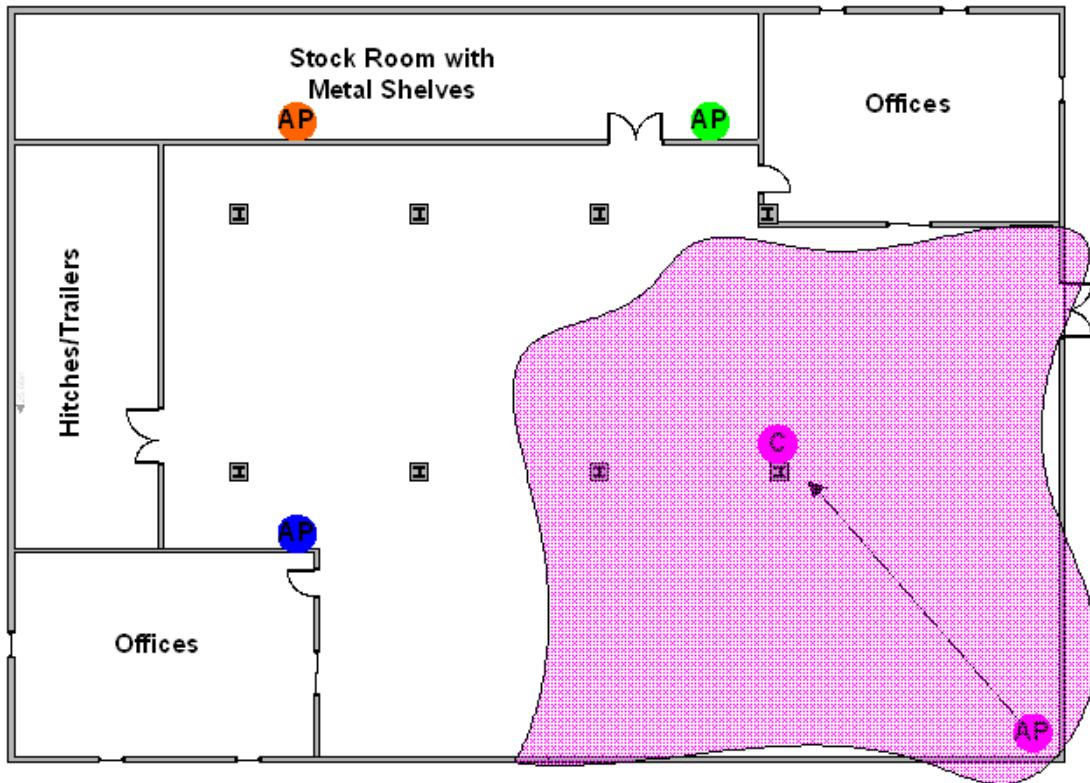
Step 5: When you reach the farthest point of connection mark the spot.   Now you move the access point to this new spot as have already determine the farthest point of the access point installation spot if wireless service is required from corner of the room.

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

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

Step 8: Repeat step 1~6 of survey on site as necessary, upon completion you will have an diagram and information of site survey. As illustrated below.
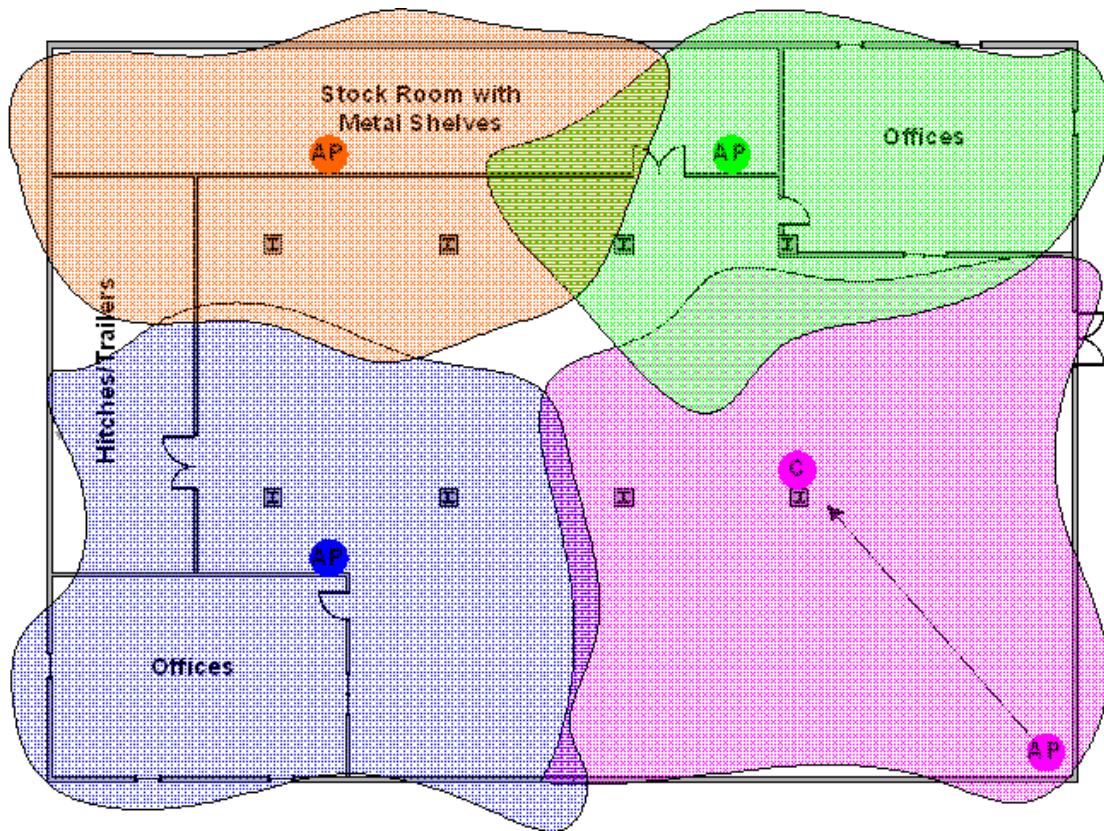
Note: If there are more than one access point is needed be sure to make the adjacent access point service area over lap one another.   So the wireless station is able to roam.   For more information please refer to roaming at

5. Configure 802.1x and WPA

- What is the WPA Functionality?
- Configuration for Access Point
- Configuration for your PC

- **What is WPA Functionality?**

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WAP and WEP are user authentication and improved data encryption. WAP applies IEEE 802.1x Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can not use the P-660HN-T1A's local user database for WPA authentication purpose since the local user database uses MD5 EAP which can not to generate keys.

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check and IEEE 802.1x. Temporal Key Integrity Protocol uses 128-bits keys that are dynamically generated and distributed by

102

the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extend initialization vector (IV) with sequencing rules and a re-keying mechanism.

If you do not have an external RADIUS, server, you should use **WPA-PSK** (WPA Pre-Share Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

Here comes **WPA-PSK Application example** for your reference.

- **Configuration for Access point**

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using local user database internal to the P-660HN-T1A (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

Step 1: To change your P-660HN-T1A's authentication settings, login Web Configurator, Advanced Setup, **Network -> Wireless LAN -> AP**

Step 2: Select **'Security Mode'** as **WAP-PSK.**

Step 3: Type the Pre Shared Key in the **Pre-Shared Key** field.

Step 4: Click **Apply** to finish.
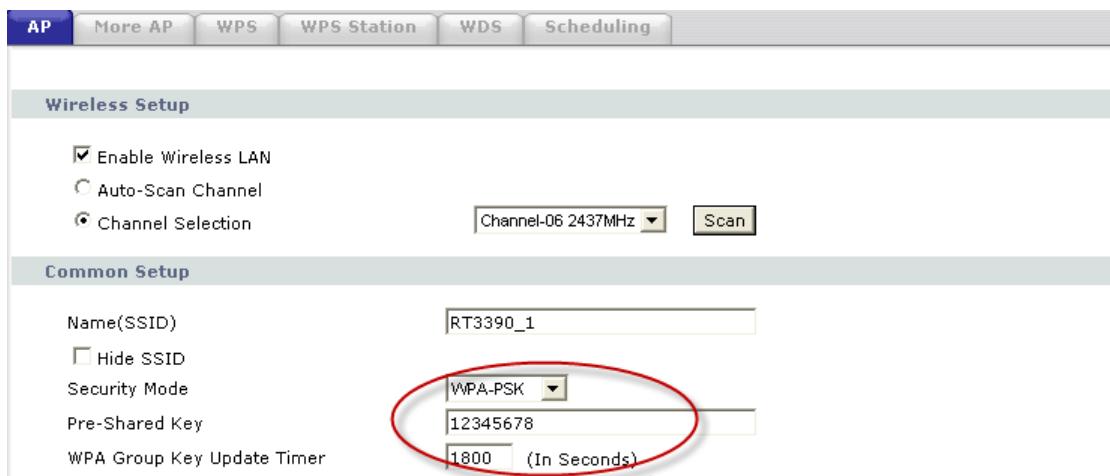
- **Configuration for your PC**

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

Step 2: Select the configuration tab, type in the SSID (Service Set Identifier), select the operating Mode as **Infrastructure,** and select proper channel.
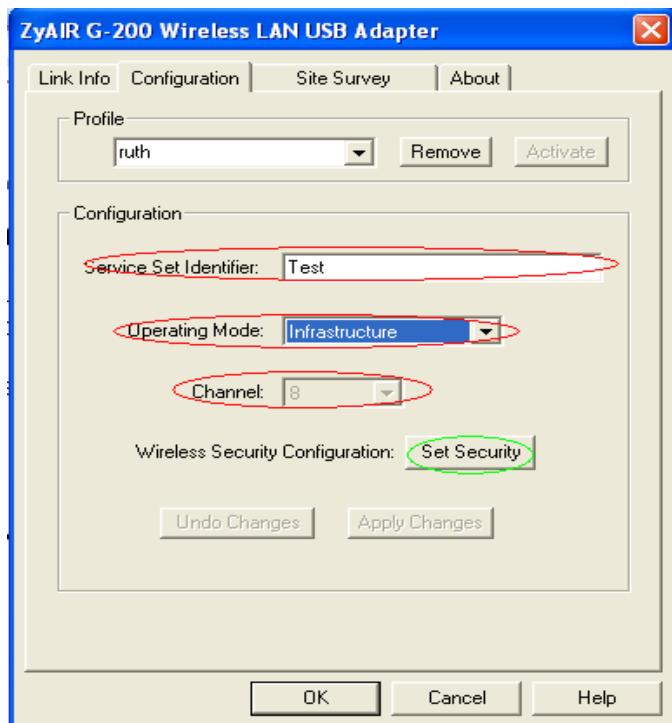

Step 3: Click Set Security to configure the security parameters:
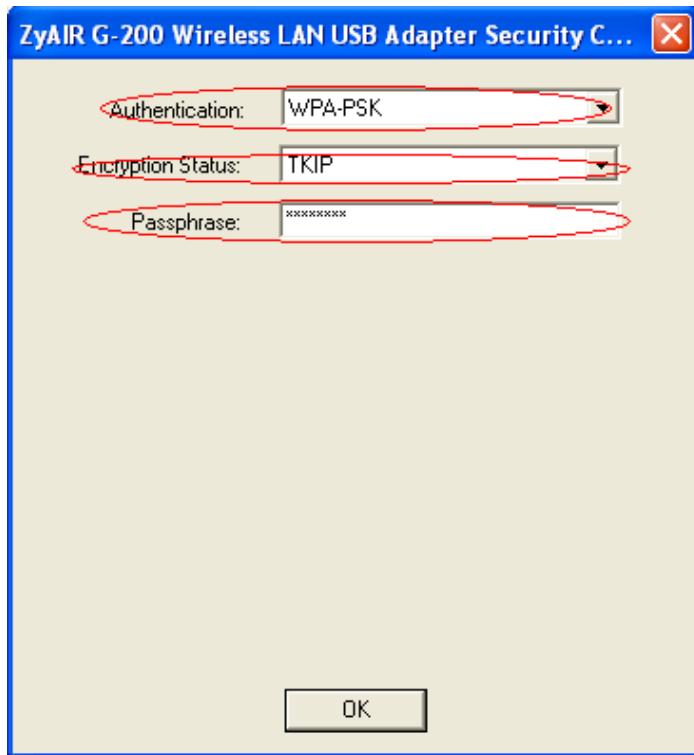
Step 4: Click OK for finish, and begin to Site survey. Connect to the AP as you have configured.
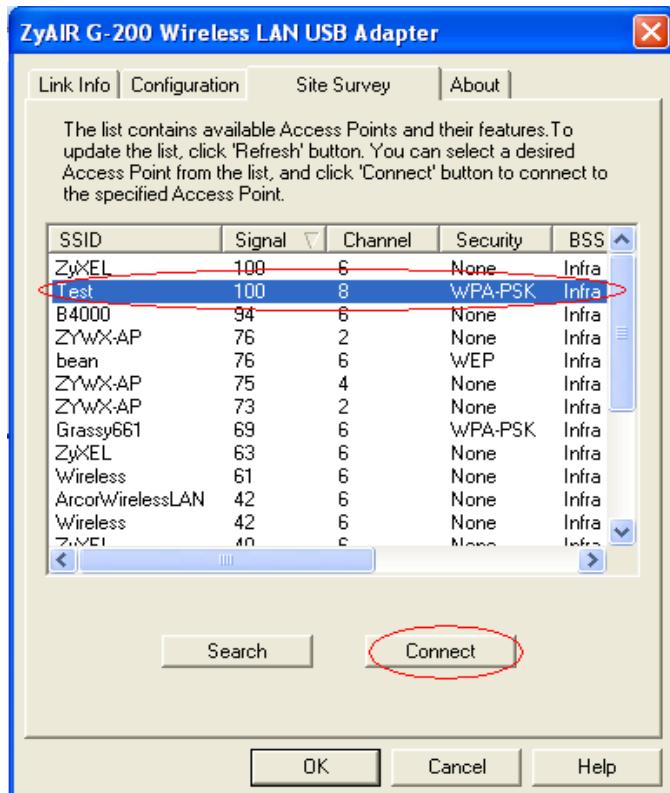
Step 5: Click Link Info tab, if the PC associated and authenticated with AP successfully, we will see the following information.
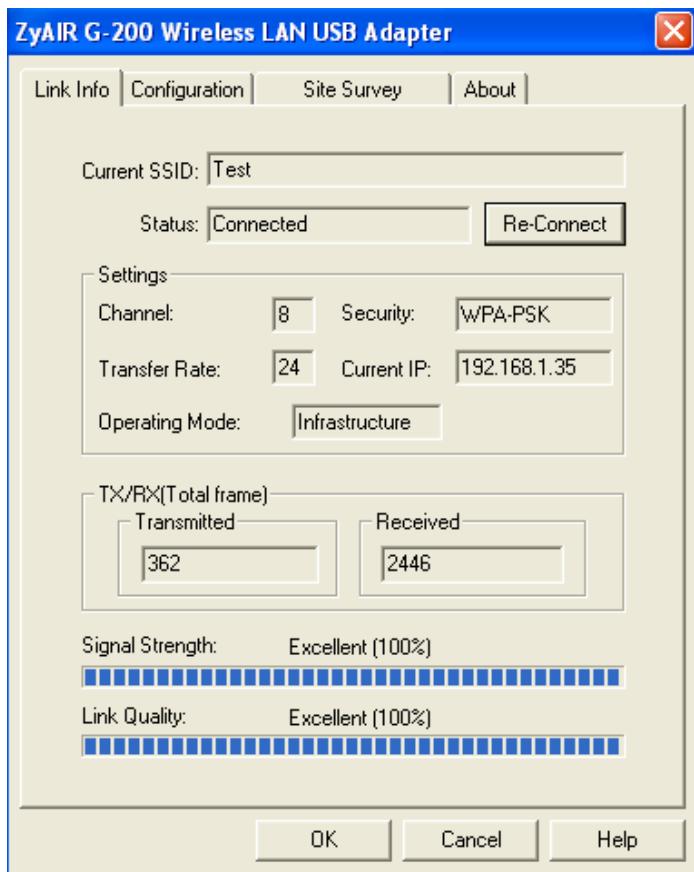
6. The WPS/WLAN Button

You can use the WPS WLAN ON/OFF button to turn the wireless LAN off or on. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

1. Turn the Wireless LAN Off or On

(1) Make sure the POWER LED is on (not blinking).

(2) Press the WPS WLAN ON/OFF button for 1 to 5 seconds and release it. The WPS/WLAN LED should change from on to off or vice versa.

2. Activate WPS

(1) Make sure the POWER LED is on (not blinking).

(2) Press the WPS WLAN ON/OFF button for 5 to 10 seconds and release it.

106

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:

```
    0 02:10:02.390 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
```

[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-660HN-T1A 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:
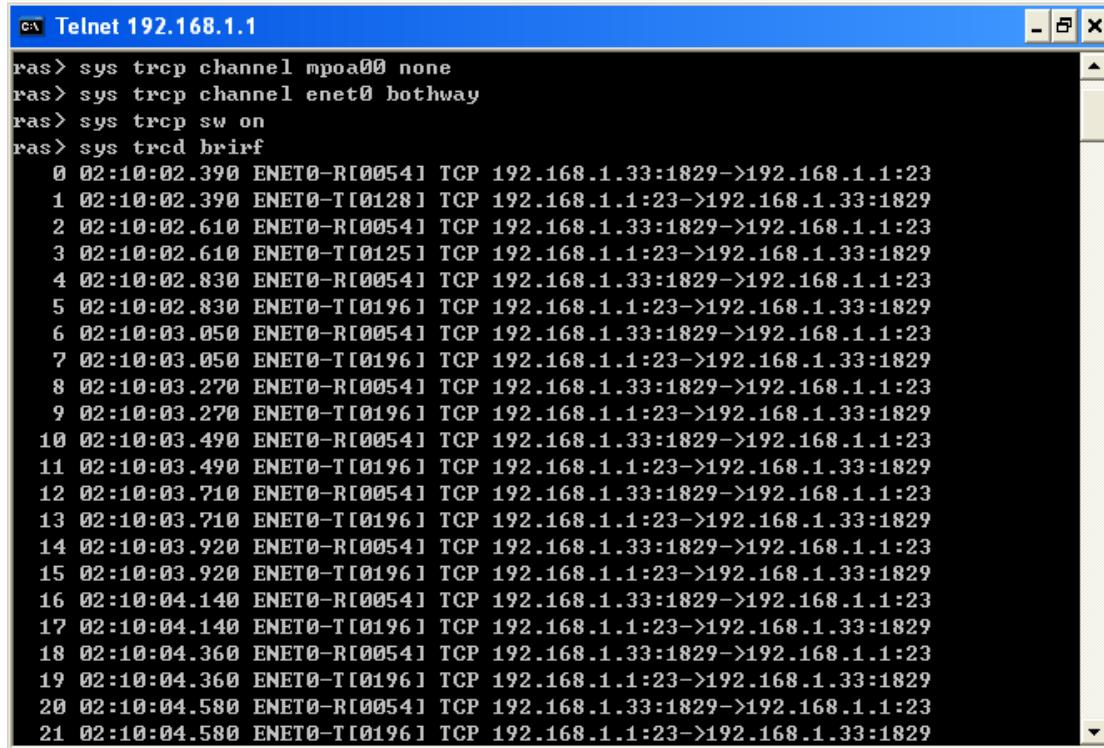
```
Telnet 192.168.1.1                                        _ 回 ×
ras> sys trcp channel mpoa00 none
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on
ras> sys trcd brirf
   0 02:10:02.390 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
   1 02:10:02.390 ENET0-T[0128] TCP 192.168.1.1:23->192.168.1.33:1829
   2 02:10:02.610 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
   3 02:10:02.610 ENET0-T[0125] TCP 192.168.1.1:23->192.168.1.33:1829
   4 02:10:02.830 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
   5 02:10:02.830 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
   6 02:10:03.050 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
   7 02:10:03.050 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
   8 02:10:03.270 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
   9 02:10:03.270 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
  10 02:10:03.490 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
  11 02:10:03.490 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
  12 02:10:03.710 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
  13 02:10:03.710 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
  14 02:10:03.920 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
  15 02:10:03.920 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
  16 02:10:04.140 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
  17 02:10:04.140 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
  18 02:10:04.360 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
  19 02:10:04.360 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
  20 02:10:04.580 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
  21 02:10:04.580 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
```

(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:

```
█ Telnet 192.168.1.1                                               _ ⊡ ×
ras> sys trcp channel enet0 none
ras> sys trcp channel mpoa00 bothway
ras> sys trcp sw on
ras> sys trcd parse
------<0000>--------------------------------------------------------
MPOA Frame: MPOA00-RECU   Size:  60/ 60   Time: 02:20:24.510
Frame Type: Ethernet Packet

  Ethernet Header:
    Destination MAC Addr      = 001349000001
    Source MAC Addr           = 000480EF2E78

    Network Type              = 0x0800 (TCP/IP)
  IP Header:
    IP Version                = 4
    Header Length             = 20
    Type of Service           = 0x00 (0)
    Total Length              = 0x0028 (40)
    Idetification             = 0x3F0F (16143)
    Flags                     = 0x02
    Fragment Offset           = 0x00
    Time to Live              = 0x71 (113)
    Protocol                  = 0x06 (TCP)
    Header Checksum           = 0x9FCD (40909)
    Source IP                 = 0xDEAC8AF3 (222.172.138.243)
    Destination IP            = 0xAC19153A (172.25.21.58)

  TCP Header:
    Source Port               = 0x0F28 (3880)
    Destination Port          = 0x2966 (10598)
    Sequence Number           = 0x326B4309 (845890313)
    Ack Number                = 0xAD825B3A (2911001402)
    Header Length             = 20
    Flags                     = 0x10 (.A....)
    Window Size               = 0x2BE6 (11238)
    Checksum                  = 0xA23B (41531)
    Urgent Ptr                = 0x0000 (0)

  TCP Data: (Length=6, Captured=6)
    0000: 00 00 00 00 00 00                            ......

  RAW DATA:
```

- **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-660HN-T1A)
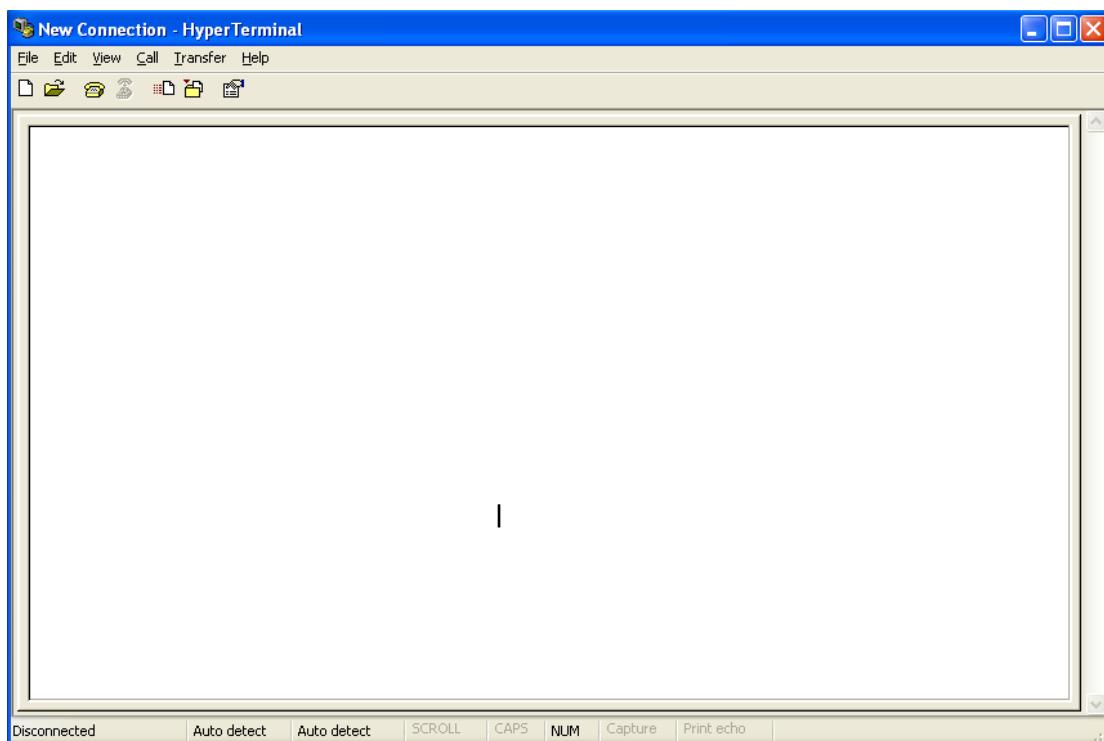
Step 2: Click the 'properties' to configure parameters to telnet to the

P-660HN-T1A.
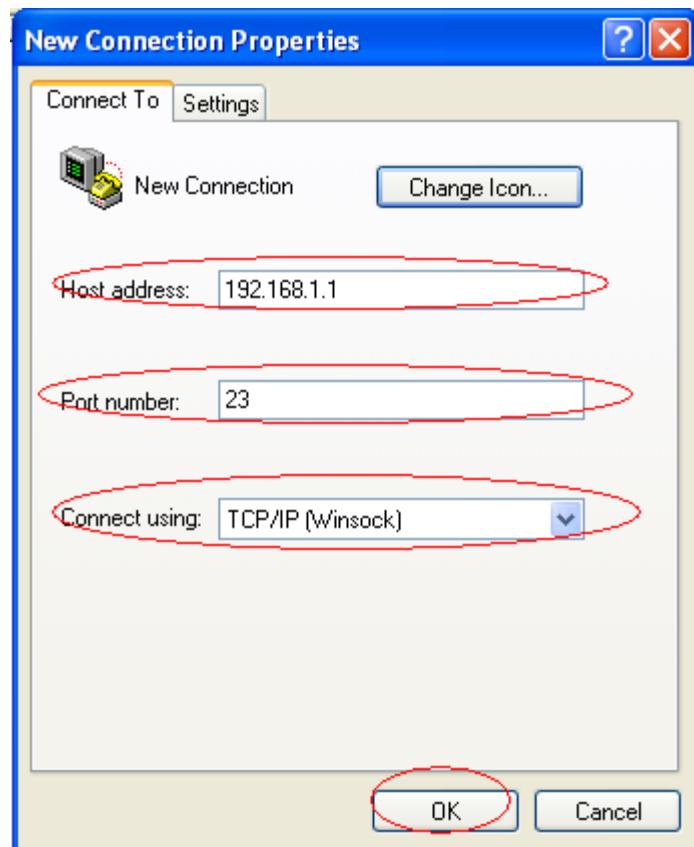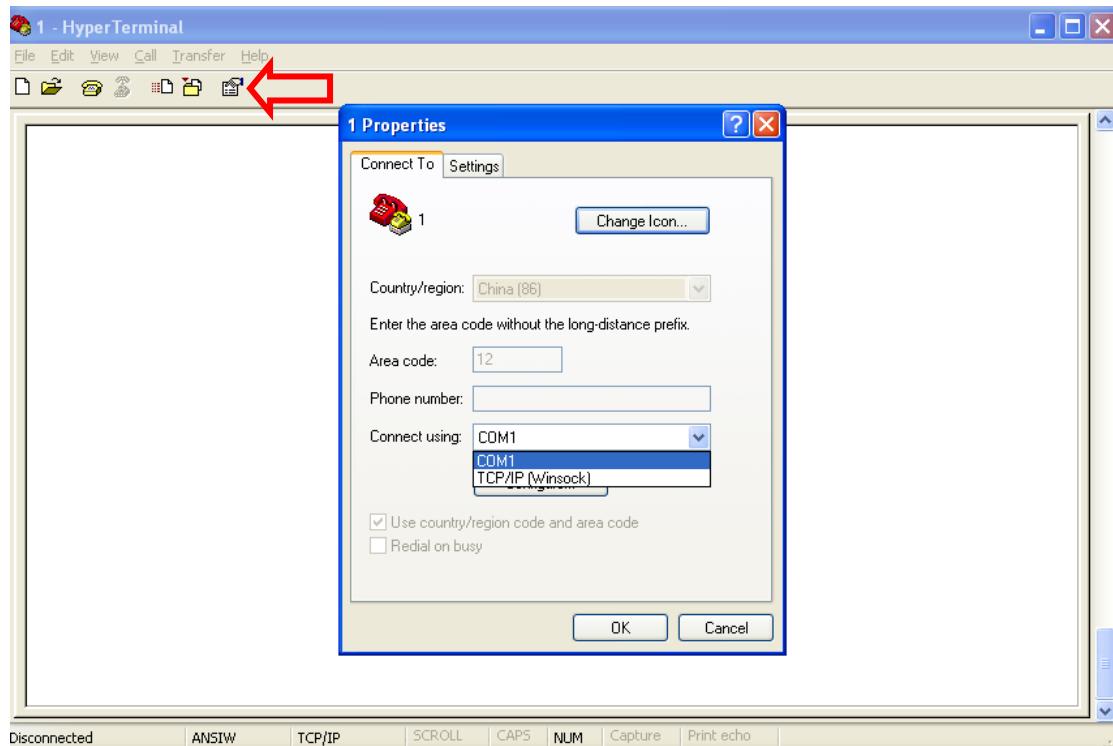
Step 3: So that after you invoke the relevant commands, you could save the

logs you've captured.
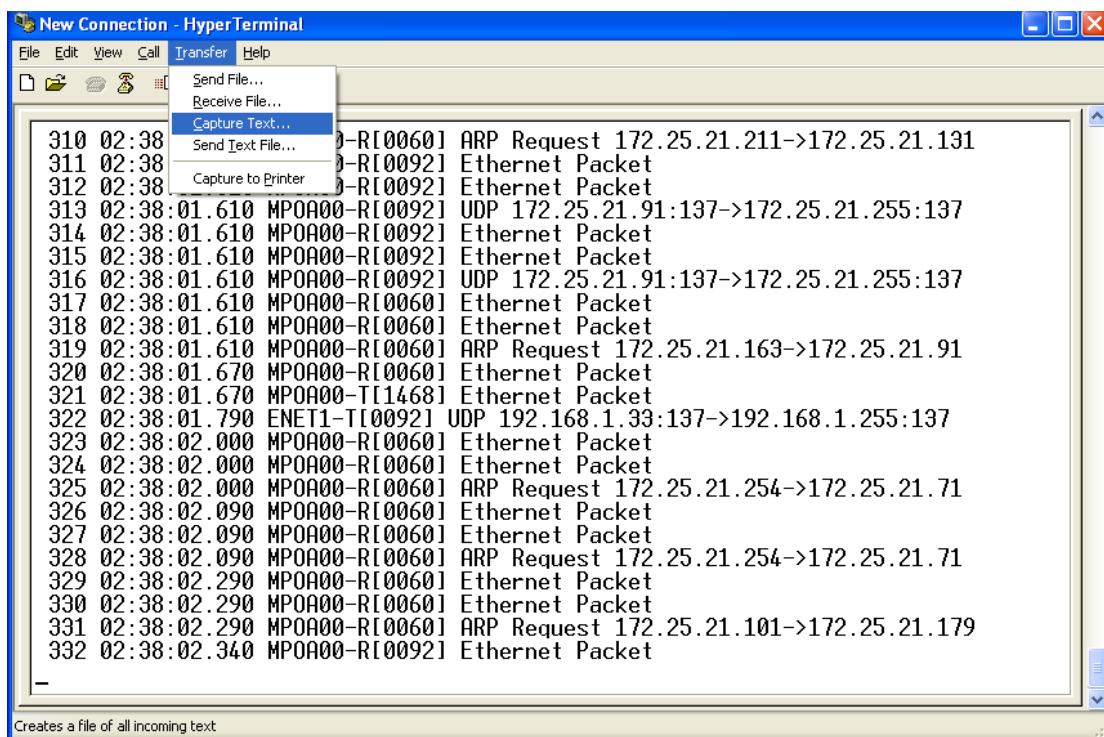
2. Firmware/Configurations Uploading and Downloading using TFTP

- **Using TFTP client software**

  - Upload/download firmware/confituration via LAN
  - Upload/download Prestige configurations via LAN

(1) Using TFTP to upload/download firmware/configuration 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:
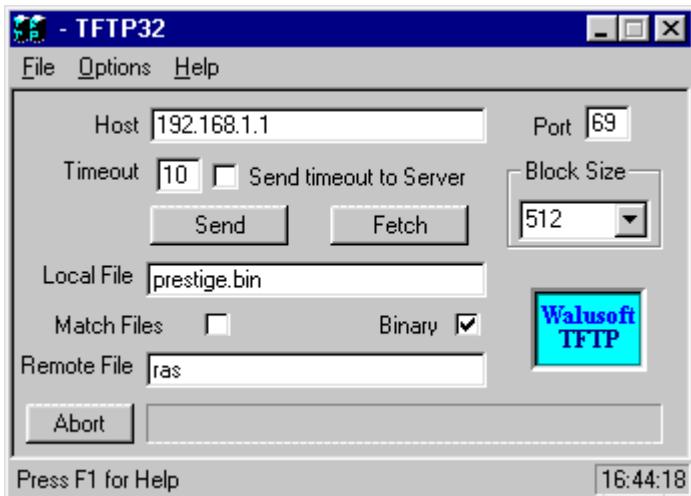
The 192.168.1.1 is the IP address of the Prestige. The local file is the source file of the firmware that is available in your hard disk. The remote file is the file name that will be saved in Prestige. Check the port number 69 and 512-Octet blocks for TFTP. Check **'Binary'** mode for file transfering.

(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-660HN-T1A configuration, please get the remote file **'rom-0'** from the Prestige.
Step 5: To upload the P-660HN-T1A configuration, please save the remote file as **'rom-0'** in the Prestige.

An example:
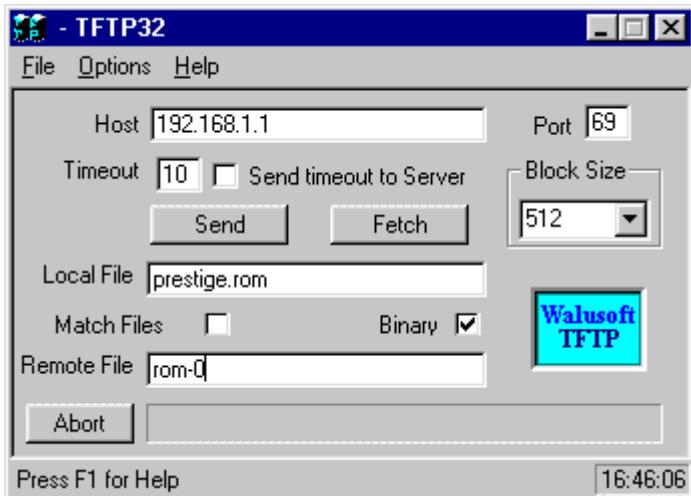
- The 192.168.1.1 is the IP address of the Prestige.
- The local file is the source file of your configuration file that is available in your hard disk.
- The remote file is the file name that will be saved in Prestige.
- Check the port number 69 and 512-Octet blocks for TFTP.
- Check 'Binary' mode for 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 via LAN : **c:\tftp -i [PrestigeIP] get ras [localfile]**
Step 4: Upload P-660HN-T1A configurations via LAN: **c:\tftp -i [PrestigeIP] put [localfile] rom-0**
Step 5: Download P-660HN-T1A 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'.
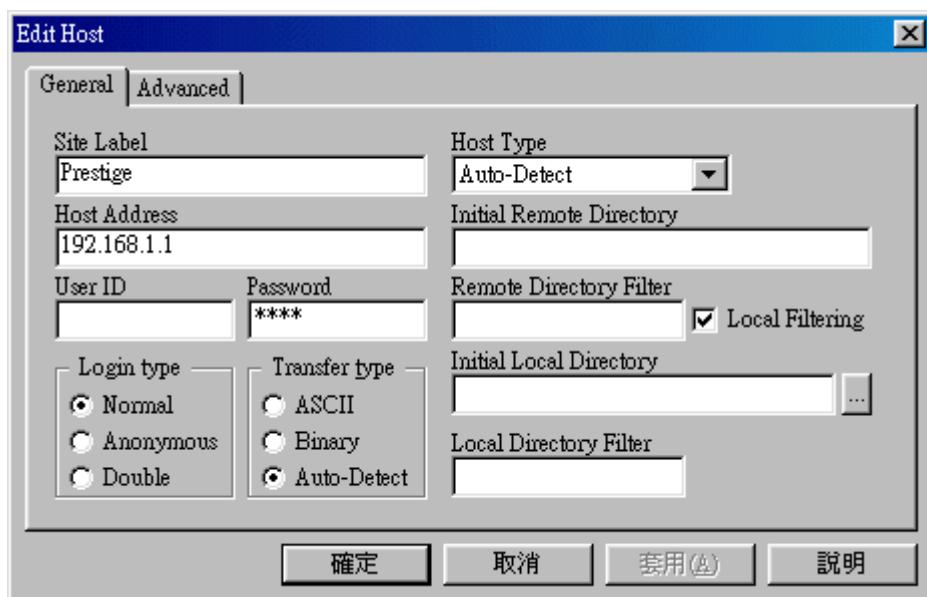
Step 2: Press **'OK'** to ignore the 'Username' prompt.

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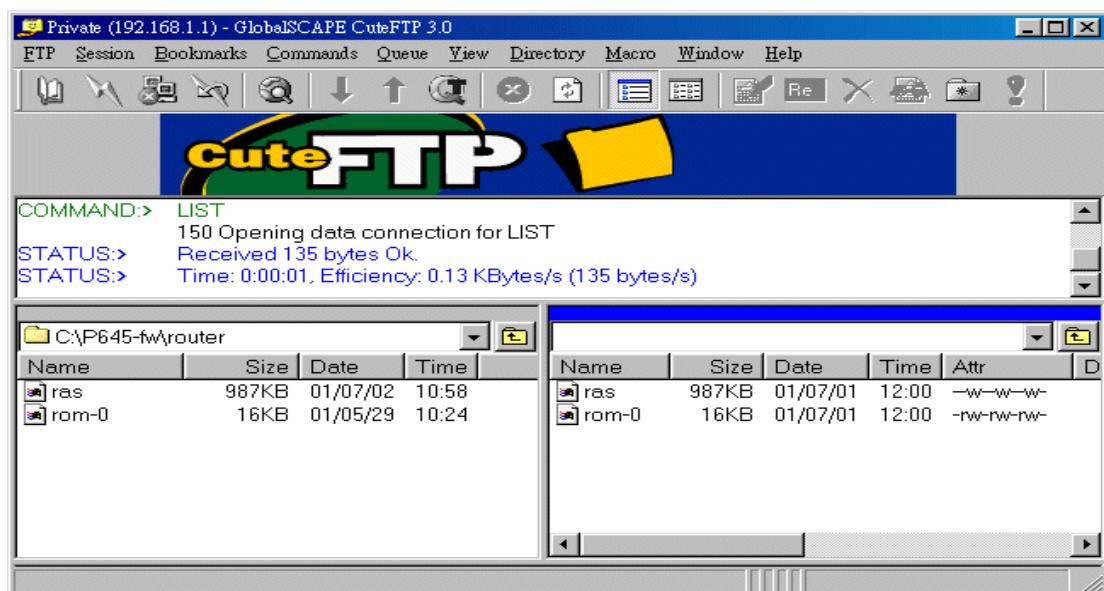
Step 4: The Prestige reboots automatically after the uploading is finished. Please do not power off the router at this moment.

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.