P-870HW-I Series

802.11g Wireless VDSL/VDSL2 4-port Gateway

Support Notes

Version1.1
Oct. 2006

FAQ

ZyNOS FAQ

1. What is ZyNOS?

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

2. How do I update the firmware and configuration files?

This can be done if you have Administrator access to your P-870HW-I. You can upload the firmware or configuration files to Prestige with the Web Configurator or FTP client software; however you CAN NOT upload the firmware or configuration file via Telnet since the Telnet connection will be dropped during the uploading process. Please do not power off the router right after the FTP uploading completes, since the router need some time to send the firmware to its flash memory.
Note: There may be firmware versions that cannot be upgraded with the Web Configurator. In this case, ZyXEL will prepare the special Upload Software for you. Please read the firmware release note carefully before uploading.

3. 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 the router to factory defaults with the following process:

Use the RESET button on the rear panel of P-870HW-I to reset the router; the LAN IP address will be reset to “192.168.1.1” and the password to “1234” afterwards.

4. How to use the Reset button?

a. Turn your P-870HW-I on. Make sure the “SYS” LED light is on (not blinking)

b. Press the RESET button for 1 to 5 seconds then release. If the “SYS” LED light begins to blink, the OTIST wireless auto security function on P-870HW-I is enabled.

c. Press the RESET button for 6 seconds then release. If the “SYS” LED begins to blink, the default configuration is restored and the P-870HW-I restarts itself immediately.

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

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

When the Prestige, acting as SUA, receives a packet destined to the Internet from a local client, 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 from a local pool. It then re-computes 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 incoming packets from the Internet are received by the Prestige, the original source IP address and TCP/UDP port numbers are written into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are re-computed, and the packet is delivered to its intended destination. This is done with a table of IP addresses and port numbers of local systems kept track by SUA.

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

When you edit a remote node in Web Configurator, Advanced Setup, **Network -> NAT -> General**, there will be two options:

- SUA Only
- Full Feature

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

The P-870HW-I now has the Full Feature NAT that 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 Full Feature NAT enables special applications such as several severs using the same port numbers on multiple global IP addresses (e.g., FTP servers using port 21/20) are allowed on the LAN for external access.

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

Yes, it is possible. Because P-870HW-I delivers packets to designated local servers by looking up to a SUA server table. To make a local server accessible to outside users, the port number and the internal IP address of the server must be configured properly. (This can be done in the Web Configurator, **Advanced Setup** > **Network > NAT > Port Forwarding**).

8. When should I choose Full Feature NAT?

To allow outside access to multiple local servers using one global IP addresses through SUA on the LAN, “visible” servers had to be mapped to different ports on the global IP. If Full Feature NAT is selected, multiple local servers (mapping to the same port or not) on the LAN are accessible from outside with multiple global IP addresses.

Supports to Non-NAT Friendly Applications

Since some Internet application servers do not allow users to login from the same IP address (such as some MIRC servers), users on the same LAN may not log into the same server simultaneously. In this case, Many-to-Many No Overload or One-to-One NAT mapping types can be selected to allow users to enter the server with unique global IP addresses.

9. 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. Details of mapping between ILA (Internal Local Address) and IGA (Inside Global Address) are described below. Here we define the local IP addresses as ILA and the global IP addresses as IGA:

- One-to-One: In the One-to-One mode, the P-870HW-I maps one ILA to one IGA.
- Many-to-One: In the Many-to-One mode, the P-870HW-I maps multiple ILAs to one IGA. This is equivalent to the Single User Account (SUA; i.e. PAT, port address translation) feature supported by older ZyNOS routers. On new Prestige routers, SUA is optional.
- Many-to-Many Overload: In the Many-to-Many Overload mode, the P-870HW-I maps multiple ILAs to shared IGAs.
- Many One-to-One: In the Many One-to-One modes, the P-870HW-I maps each ILA to a unique IGA.

- Server: In the Server mode, the P-870HW-I maps multiple local servers to one global IP address. This allows useDrs to specify multiple servers of different types behind the NAT for external access. Note: if each server needs mapping 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

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

By factory default, the Prestige does not limit the number of the users but the number of sessions. It can be configured it in the Web Configurator, Advanced Setup **Network -> NAT -> General**. In addition, the “ip nat session [session per host]” command in SMT menu 24.8 can be used as well.

Product FAQ

1. How can I manage P-870HW-I?

- Embedded Web GUI for local and remote management
- CLI (command-line interface)
- Telnet support for remote configuration change and status monitoring
- FTP sever, firmware upgrade and configuration backup/restore are supported

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

The factory default password for the Web Configurator is “1234”.

You can change the password after logging into the Web Configurator. Please keep your new password on record whenever you change it to prevent system lock-up by wrong passwords.

3. How do I know P-870HW-I's WAN IP address assigned by the ISP?

There are two methods to check the WAN IP address assigned by ISP.

In Web Configurator, see "IP address: x.x.x.x" shown on the “Status” page.

In SMT menu, you can find the system status in menu 24.1.

4. What is the micro filter or splitter for?

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

5. How do I know I am using PPPoE?

PPPoE requires a user account to log into the provider's server. If you need a set of user name and password to connect to the ISP, you are probably using PPPoE. If you can simply connect to the Internet when you turn on the computer, you are probably not using PPPoE. You can also check your ISP or the information sheet given by the ISP. Please choose “PPPoE” as the encapsulation type in the P-870HW-I if you use PPPoE for ISP connection.

6. Why does my provider use PPPoE?

Since PPPoE emulates a dial-up connection, it allows an ISP to provide broadband services over its existing network configuration. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management, etc.

7. What is DDNS?

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

Without DDNS, only the WAN IP of the P-870HW-I can be used to reach internal servers; however it’s inconvenient if this IP is dynamic. With DDNS supportE, P-870HW-I users can apply for a DNS names (e.g., www.zyxel.com.tw) for each server (e.g., Web server) from any DDNS server. Outside users can always access the EWeb server using the www.zyxel.com.tw regardless of the WAN IP of the P-870HW-I.

When the ISP assigns the P-870HW-I a new IP, the P-870HW-I will send the new IP address to the DDNS server for it to update its IP-to-DNS entry. Once the IP-to-DNS table on the DDNS server is updated, the DNS name for your Web server (i.e., www.zyxel.com.tw) is still usable.

8. When do I need DDNS service?

If you wish your internal servers to be reached by DNS names instead of the dynamic IP addresses, DDNS service can be used. The DDNS server can map a dynamic IP address to a static hostname. When the ISP assigns a new IP, the P-870HW-I can send this IP to the DDNS server for it to update.

9. What is DDNS wildcard? Does the P-870HW-I support DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the "*.yourhost.dyndns.org" hostname to be mapped to the same IP address as "yourhost.dyndns.org", for instance. This feature is useful when there are multiple servers inside the LAN, and you wish visitors to use URLs like "www.yourhost.dyndns.org" to reach your hosts.

Yes, the P-870HW-I supports DDNS wildcard that DynDNS.org supports. When wildcard is needed, simply enter "yourhost.dyndns.org" in the Host field in the Web Configurator, Advanced Setup **Maintenance -> System -> Dynamic DNS**.

10. Can P-870HW-I's SUA handle IPSec packets sent by the IPSec gateway?

Yes, P-870HW-I's SUA can handle the IPSec ESP Tunneling mode. When packets go through SUA, SUA will change the source IP address and source port for the host. To pass IPSec packets, SUA must analyze the ESP packet with protocol number 50, replace the source IP address of the IPSec gateway to the router's WAN IP address. However, SUA should not change the source port of the UDP packets used for key managements. Since the remote gateway checks this source port during connections, the port thus cannot be changed.

11. How do I setup my P-870HW-I for routing IPSec packets over SUA?

For outgoing IPSec tunnels, no extra setting is required.

For forwarding the inbound IPSec ESP tunnel, A "Default" server set is required. You could configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding -> Default Server Setup**:
It is because that SUA makes your LAN appear as a single machine to the outside world, and the LAN users are invisible to outside users. To make an internal server available for outside access, we must specify the service port and the LAN IP of this server in Web Configurator. As such SUA is able to forward the incoming packets to the requested service behind SUA, and outside users can access the servers with P-870HW-I's WAN IP address. So we have to configure the internal IPsec client as a default server (unspecified service port) when it acts as a server gateway.

12. 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 certain specified key words in the URL. You can set a schedule for P-870HW-I to perform content filtering, or specify trusted IP addresses on LAN to prevent P-870HW-I from filtering. You can configure the details in Web Configurator, Advanced Setup, **Security -> Content Filter**.

VDSL FAQ

1. How does VDSL compare to Cable modems?

VDSL provides a dedicated service over a single telephone line; cable modems offer a dedicated service over a shared media. Cable modems' 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 VDSL, 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 VDSL 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 20Mbps data rate on 5Kft and 100Mbps data rate on 700ft using the 26AWG loop. The shorter the loop, the better the throughput.

3. What is the micro filter used for?

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

4. How do I know the VDSL line is up?

You can see the DSL LED Green on the P-870HW-I's front panel is on as the VDSL physical layer is up.

5. How does the P-870HW-I work on a noisy VDSL?

Depending on the line quality, the P-870HW-I uses “Fall Back” and “Fall Forward” techniques to automatically adjust the date rate.

6. How do I know the details of my VDSL line data rate?

You can refer to these information in Web Configurator, Advanced Setup, **Status -> Interface Status**.

7. What are the signaling pins of the VDSL connector?

The signaling pins on the P-870HW-I's VDSL connector are pin 3 and pin 4. The two pins in the middle are for the RJ11 cable.

8. What is triple play?

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

- The different services (such as video, VoIP and Internet access) require different Quality of Service.
- The Voice (VoIP) data has the highest priority.
- The Video (IPTV) data has medium priority.
- Regular Internet data access, such as FTP, has the lowest priority.

Triple Play is a protocol-based policy to forward packets from LAN port to destination, thus you can configure each protocol (SIP and FTP predefined by factory default) separately to assign different QoS to different applications. This can be done manually in Web Configurator, Advanced Setup, **Management -> Bandwidth MGMT -> Configuration.**

Firewall FAQ

General

1. What is a network firewall?

A firewall is a system or a 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. A firewall consists of two mechanisms: One blocks undesirable traffics, and the other permits desirable traffics.

2. What makes P-870HW-I secure?

The P-870HW-I is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND attack, IP Spoofing, etc. It also uses Stateful Packet Inspection (SPI) to determine if an inbound connection is allowed through the firewall to the private LAN. The P-870HW-I 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 Firewalls
2. Application-Level Firewalls
3. Stateful Inspection Firewalls

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 are generally hosts running proxy servers that prevents direct traffics between networks and performs logging and auditing of passing traffics. A proxy server is an application gateway or circuit-level gateway that runs on top of general operating systems such as UNIX or Windows NT. It hides valuable data by requiring users to communicate with secure systems via a proxy, but has a key drawback of lower 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 integrity of the connection and to adapt to dynamic protocols. The flexible nature of Stateful Inspection firewalls generally provides the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support.

4. What kind of firewall is the P-870HW-I?

1. The P-870HW-I firewall inspects packet contents and IP headers. It is applicable to all protocols that understand data in the packet is intended for other layers, from network layer up to the application layer.
2. The P-870HW-I 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-870HW-I firewall uses session filtering, i.e. the smart rules that enhance the filtering process and control the network session rather than controlling individual packets in a session.
4. The P-870HW-I 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-870HW-I firewall provides email service to notify administrators for routine reports and emergency alerts.

5. Why do you need a firewall when your router has 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 NAT restrict access to particular computers and networks, however, for some companies this security may be insufficient since packets filters typically cannot maintain session state. Thus a firewall should be considered for greater security.

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 oversized packet is then sent to an unsuspecting system. This may cause a system to 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 into smaller chunks, while 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 may crash, hang or reboot.

9. What is SYN Flood attack?

SYN attack floods a targeted system with a series of SYN packets, and each packet causes the targeted system to issue a SYN-ACK response. When 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 (such as “Smurf”) attack exploits an IP specification feature known as directed or subnet broadcasting to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address with packets of the network’s broadcast address, then the router would 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, rendering communications impossible.

12. What is IP Spoofing attack?

Many DoS attackers also use IP Spoofing as part of their attempt. 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 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-870HW-I?

There are two default ACLs pre-configured in the P-870HW-I; 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 P-870HW-I firewall?

You can use the Web Configurator to configure the P-870HW-I firewall. By factory default, you can connect a PC to the LAN Interface of P-870HW-I and access its Web Configurator with the “http://192.168.1.1” URL.
Note: Don’t forget to enter the Administrator Password.

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

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

1. Change the default Administrator password required when setting up the firewall.
2. Limit the access privilege to the Web Configurator or CLI of your P-870HW-I. You can enter the IP address of a secured LAN host in Web Configurator, Advanced Setup, **Management -> Remote MGNT -> [WWW] ->Secured Client IP Address** to allow access to your P-870HW-I.

The default value is “All”, meaning any host can connect to your P-870HW-I via Telnet or access the Web Configurator.

3. Why can't I configure my P-870HW-I using Web Configurator/Telnet over WAN?

There are three reasons that WWW/Telnet connection 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 the following.
WWW (For accessing the Web Configurator):
Source IP= Remote trusted host **Destination IP**= router' WAN IP **Service**= TCP/80 **Action**=Forward
TELNET (For accessing the 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, **Management -> Remote MGNT**:

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

4. Why can't I upload the firmware or 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 the following.

Source IP= FTP host **Destination IP**= P-870HW-I's WAN IP **Service**= FTP TCP/21, TCP/20 **Action**=Forward.

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

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

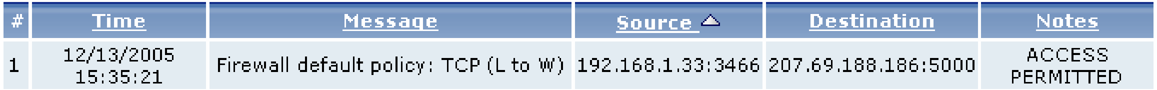
Log and Alert

1. When would P-870HW-I generate the firewall log?

The P-870HW-I 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 the Web Configurator.

2. What's in the firewall log?

The log supports up to 128 entries and there are 5 columns in 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-870HW-I, including firewall logs and system logs, will be moved to the centralized logs for users to look up: Web Configurator, Advanced Setup, **Maintenance -> Logs ->View Log**.
The log keeps 128 entries, and new entries will overwrite the old ones if the log generates more entries.
Before viewing the firewall logs, there are two steps you need to do:

(1) Enable log function in Centralized logs setup via following methods,

- Web configuration: Advanced Setup, **Maintenance -> Logs -> Log Settings**, check Active logs and Alter options depending on the actual situation.
- SMT: Use the "**sys logs syslog active 1**" command in menu 24.8 to active logs and alter options.

(2) Enable log function in the default firewall policy or in firewall rules.
After the above two steps, you can view firewall logs via following methods,

- Web Configurator: Advanced Setup, **Maintenance -> Logs ->View Log**.
- SMT: Use the "**sys logs display**" command in menu 24.8 to view the logs.

You can also view the Centralized logs via mail or syslog. Please configure the mail server or Unix Syslog server in Web configuration: Advanced Setup, **Maintenance -> Logs -> Log Settings**.

4. When do the P-870HW-I generate the firewall alert?

The P-870HW-I generates alerts and optionally sends them via email when an attack is detected by the firewall. To enable alert emails, you must configure the email server and address using Web Configurator, Advanced Setup, **Maintenance -> Logs -> Log Settings**. You can also specify the frequently of the alert emails.

5. What is the difference between log and alert?

A log entry is just added to the log inside the P-870HW-I and emailed along with all other log entries at the scheduled time. An alert is sent 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 air. Typical bit rates are 11Mbps and 54Mbps, although in practice data throughput is half of these. Wireless LANs can be established simply by installing wireless NICs on PCs. If connection to a wired LAN is required, an Access Point (AP) is used as a bridging device. APs are typically located close to the centre of the wireless client population.

2. What are the advantages of Wireless LAN?

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

Installation Speed and Simplicity: Installing a wireless LAN system is fast and easy and it eliminates the need to run cables through walls and ceilings.

Installation Flexibility: Wireless technology allows the network to cover where wires can't.

Lower Cost-of-Ownership: While the initial investment required for wireless LAN hardware can be higher than the wired setting, overall installation expenses and lifecycle 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 can be easily changed, and wireless networks are scalable from peer-to-peer networks suitable for a few users to a full infrastructure allowing thousands of users to roam in a large area.

3. What is the disadvantage of Wireless LAN?

The speed of a wireless LAN is still relatively slower than a wired one. And since it involves wireless access points and LAN cards that cost more than wired hubs and CAT-5 cables, setting up a wireless LAN is relatively expensive.

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 a wireless server that transmits information to and from a wired Ethernet connection with one or more antennas using radio signals. An AP typically acts as a bridge for its clients to pass information to wireless LAN cards installed in computers or laptops, allowing those computers to connect to the local network or Internet without wires.

6. What's the difference between IEEE 802.11a/b/g?

The IEEE 802.11 is a wireless LAN industry standard, and the objective of IEEE 802.11 is to make sure that wireless LAN devices from different manufacturers can talk to each other. Below is a brief comparison of IEEE802.11 a/b/g standards:

	Publish Time	Frequency Band(GHZ)	Data Rate(Mbps)	Compatibility
IEEE802.11a	1999	UNII Band 5.15~5.825	6,9,12,18,24,36,48, 54	Only work with 802.11a devices
IEEE802.11b	1999	ISM Band 2.4~2.4835	1,2,5.5,11	
IEEE802.11g	2001	ISM Band 2.4~2.4835	6,9,12,18,24,36,48, 54	Backward compatible with 802.11b devices

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

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

8. 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.

9. 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.

10. Does the 802.11 interfere with Bluetooth device?

When different devices are being operated in the same frequency band, potential interference may occur. Although both 802.11b/g and Bluetooth devices occupy the same 2.4-to-2.483 GHz unlicensed frequency range, a Bluetooth device may not interfere with 802.11 devices as much as another 802.11 node. While more collisions are possible with the presence of a Bluetooth device, they could come from another 802.11 device, or a new 2.4 GHz cordless phone for that matter. However, since Bluetooth devices are usually low power, serious effects a Bluetooth device may have on an 802.11 network are unlikely, if any.

11. Can radio signals pass through walls?

Transmitting through a wall is possible depending upon the material used in its construction. In general, metals and substances with high water content do not allow most 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 reinforcement used.

12. What are the 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, e.g. microwaves, monitors, electric motors, etc.

(4) Add additional APs if necessary.

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

WLANs are generally privately owned wireless systems deployed in a corporation, warehouse, hospital or educational campus, where 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 usually operated by service providers or carriers that to offer low data rate, charge-by-usage services. Specialized applications are characteristically designed around short, burst messaging.

14. Can I manually swap the wireless module without damaging any hardware?

Yes, doing so will not harm the hardware, however the module cannot be detected or work right after being inserted to the slot; the router has to be rebooted to re-initialize the module.

15. What wireless security modes does P-870HW-I support?

P-870HW-I supports the following wireless security modes: Static WEP, WPA-PSK, WPA, 802.1x+Dynamic Key, 802.1x+Static Key, 802.1x+No Key WPA2-PSK and WPA2.

16. What Wireless standards does P-870HW-I support?

It supports IEEE 802.11b/g standards.

17. Does P-870HW-I support MAC filtering?

Yes, it supports MAC filtering of up to 32 addresses.

18. Does P-870HW-I support auto rate adoption?

Yes, it means that the AP on P-870HW-I will automatically adapt to a lower speed when client devices move beyond the optimal range, or signal interference is present. If the device moves back within the range and allows 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 nodes 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 utilize the relay feature of access points.

3. How many access points are required in a given area?

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

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

DSSS spreads its signal continuously over a wide frequency band, and it 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 unsynchronized receiver an FHSS transmission appears to be short-duration impulse noise. The 802.11 protocol can take advantage of both FHSS and DSSS.

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

No, if the antenna is optimally designed for 2.4GHz operation. WLAN NICs often include an internal antenna that would provide sufficient reception.

7. Why the 2.4 GHz frequency range?

This frequency range has been set aside by FCC and is generally labeled as “ISM band”. A few years ago Apple Computer 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 has been populated with low-power industrial, scientific and medical devices; and they may have potential interference with each other.

8. What is Server Set ID (SSID)?

SSID is a configurable identification that allows wireless clients to communicate with 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. From the security viewpoint, SSID acts as a simple shared password between base stations and clients.

9. What is an ESSID?

ESSID stands for “Extended Service Set Identifier” that identifies a wireless LAN. The ESSID of a mobile device must match the ESSID of an AP to initiate communication. The ESSID is a string of up to 32 characters and is case-sensitive.

Security FAQ

1. How do I secure the data on the radio link of P-870HW-I Access Point?

To secure the date on the radio link of P-870HW-I Access Point, any of the following security modes can be selected: Static 64/128 bit WEP, WPA-PSK, WPA, 802.1x+Dynamgic Key, 802.1x+Static Key, 802.1x+No Key, WPA2-PSK, WPA2.

2. What is WEP?

It stands for “Wired Equivalent Privacy”. WEP is a security mechanism defined within the 802.11 standard designed to raise the security of wireless network to the cable (wire) level. WEP data encryption aims to prevent unauthorized access to the network as well as eavesdropping to the wireless traffics. WEP allows the administrator to define a set of respective ”keys” for each wireless network user to pass through the WEP encryption algorithm with a “key string”. Access from anyone who does not have an assigned key will be denied. Note: WEP has been found to have fundamental flaws in its key generating process.

3. What is WPA?

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. The local user database in P-870HW-I cannot be used for WPA authentication, since the database uses MD5 EAP that is unable 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 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 to be 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. Please refer to the User Guide for more information.

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

40-bit WEP and 64-bit WEP are of the same encryption level and can interoperate. The lower level of WEP encryption uses a 40-bit (10 Hex character) as the “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 while others refer 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. The 128-bit WEP will not communicate with 64-bit WEP. Although 128-bit WEP also uses a 24-bit Initialization Vector, however it uses a 104-bit string as the secret key. Users need to employ the same encryption level in order to establish a connection.

7. Can SSID be encrypted?

No, WEP only encrypts the data packets, not the 802.11 management packets. The SSID is in the beacon and probe management messages, and goes over the air in plain text. This makes acquiring the SSID easy by sniffing 802.11 wireless traffics.

8. If SSID broadcast is turned off, can someone still sniff the SSID?

Many access points have SSID broadcasting turned on by default, so sniffers can find the SSID in the broadcast beacon packets; that is, turning off SSID broadcast in the beacon message (a common practice) cannot prevent the acquisition of SSID. Since the SSID is sent unencrypted in the probe message when a client tries to connect to an access point, a sniffer just can just wait to see the SSID when a valid user communicates with the wireless network.

9. What are Insertion Attacks?

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

10. What is a Wireless Sniffer?

An attacker that “sniffs” and captures legitimate network traffic. As many Ethernet sniffer tools capture 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 sometimes initiate attack with the same technique.

11. What is OTIST? How do I use it?

OTIST is acronym for ZyXEL’s “One Touch Intelligent Security Technology”. It enables P-870HW-I and ZyXEL’s OTIST-supported Wireless adapters to establish connections in the WPA-PSK security mode automatically with just one touch at the reset button on rear panel.

To activate the OTIST function on P-870HW-I, press the reset button for 1 to 5 seconds. The P-870HW-I will enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. The default setup key for OTIST is “01234567”.

Application Notes

General Application Notes

1. Internet Access Using P-870HW-I

In most homes, more than one computer accesses the Internet using only one Internet access account. To do this, an Internet sharing device (such as a router) is required.

ZyXEL's P-870HW-I is a VDSL modem with an integrated router.

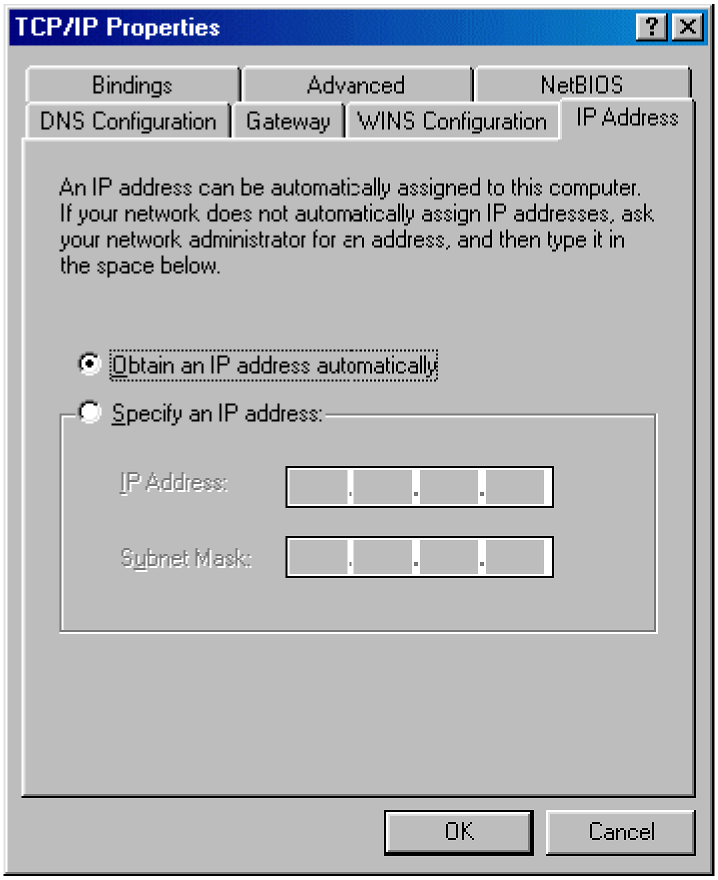
Setting up your computer

(1) Ethernet connection

Use Ethernet cables to connect your computers to the LAN ports on the P-870HW-I.

(2) TCP/IP configuration

By default, DHCP server is enabled on the P-870HW-I. You need to configure your computers as DHCP clients that obtain IP addresses from the P-870HW-I. For example, in Windows, select the "Obtain an IP address automatically" options in TCP/IP setup. An example screen is shown below. Through DHCP, the P-870HW-I also provides DNS server information if available.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

Setting up your P-870HW-I

The following procedure shows you how to use the web configurator to set your P-870HW-I in routing mode.

(1) Configure P-870HW-I Internet access settings in the web configurator. Click **Advanced Setup > Network > WAN > Internet Connection**.

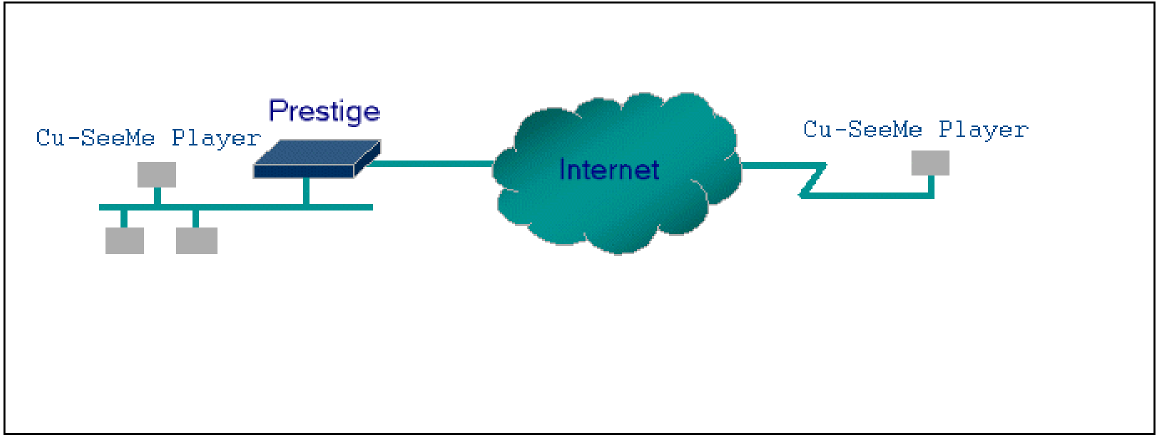
Key Settings:

Option	Description
Encapsulation	Select the correct encapsulation type that your ISP supports. For example, PPPoE.
IP Address Assignment	Set to Dynamic if the ISP provides an IP address for the P-870HW-I dynamically. Otherwise, set to Static and enter the IP address in the IP Address field.
WAN MAC Address	Select to enable or disable the Spoof WAN MAC Address feature.

(2) Set the LAN IP address for the P-870HW-I and the DHCP settings. Click **Advanced Setup > Network > LAN**.

2. 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-870HW-I. In such case, an SUA server must be configured to forward the incoming packets to the actual destination behind SUA. After the required server is configured in web configurator (**Advanced Setup > Network > NAT > Port Forwarding**) the internal server or client applications can be accessed by using the P-870HW-I's WAN IP Address.

SUA Table

The following table lists the required SUA settings for the various applications in **Advanced Setup > Network > NAT > Port Forwarding**.

ZyXEL SUA Support Table[1]

Application	Required Settings for 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, set Default/Client IP	.
Windows PPTP	None	1723/client IP
ICQ 99a	None for Chat. For DCC, set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds.	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	4662 - 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 makes your LAN 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 (ports 7648 and 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 cannot distinguish between local users using the same public IP address.

[4] Certain Quake servers do not allow multiple users to log in using the same IP address, so only one Quake user will be allowed in this case. Moreover, when a Quake server is configured behind SUA, P-870HW-I will not be able to provide information of that server on the Internet.

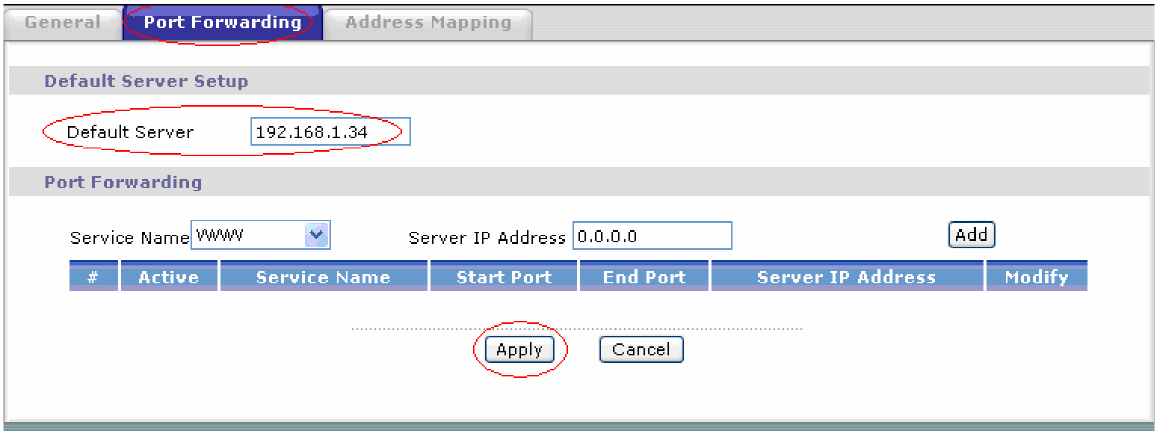
[5] Quake II has the same limitations as that of Quake I.

[6] P-870HW-I supports MSN Messenger 4.6/ 4.7/ 5.0/… video/ voice pass-through NAT. In addition, for Windows OSes that supported UPnP (Universal Plug and Play), such as Windows XP and Windows ME, UPnP support in P-870HW-I is an alternative solution to pass through MSN Messenger video/ voice traffic. For more detail, please refer to UPnP application note.

[7] P-870HW-I supports Microsoft Xbox Live with factory default configuration.

Configurations

For example, if the workstation operating Cu-SeeMe has an IP address 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-870HW-I's WAN IP address which can be obtained from the web configurator (Status > **Device Information >WAN Information**).



Default Server Setup

Default Server: 192.168.1.34

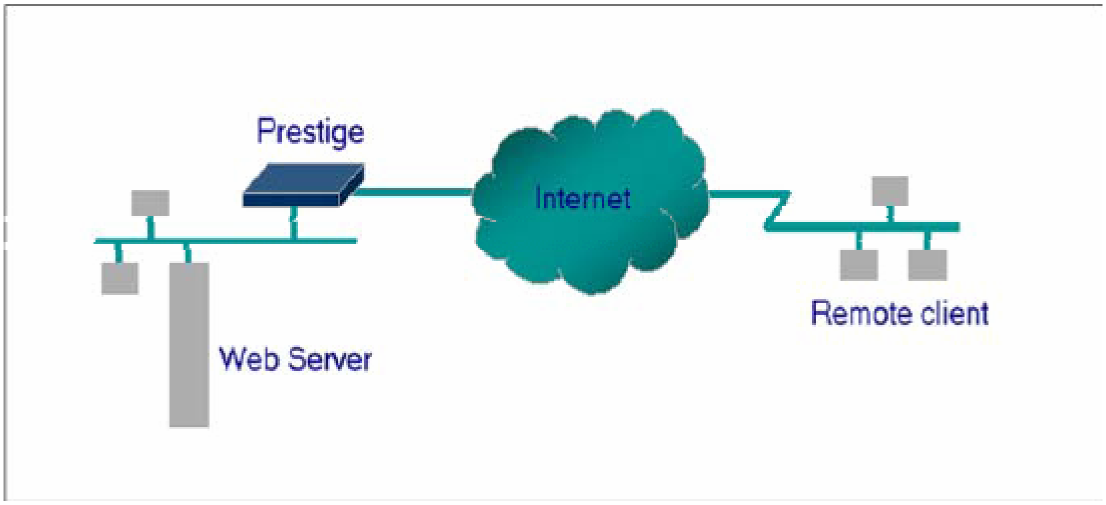
Port Forwarding

Service Name: WWW   Server IP Address: 0.0.0.0

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

Apply

Configuring an Internal Server behind SUA



Introduction

You can make internal servers (such as 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 a port number. Also, since you need to specify the IP address of a server behind the P-870HW-I, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time P-870HW-I 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.

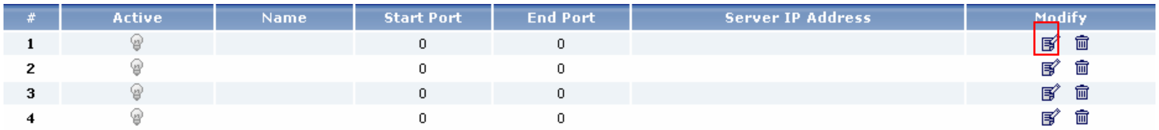
Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server. In the web configurator, click **Advanced Setup > Network > NAT > Port Forwarding**. The outside users can access the local server using the P-870HW-I's WAN IP address which can be obtained in the **WAN Information** screen (click **Status > Device Information > WAN Information**).

For example:

Configuring an internal web server for outside access (suppose the server IP address is 192.168.1.10).

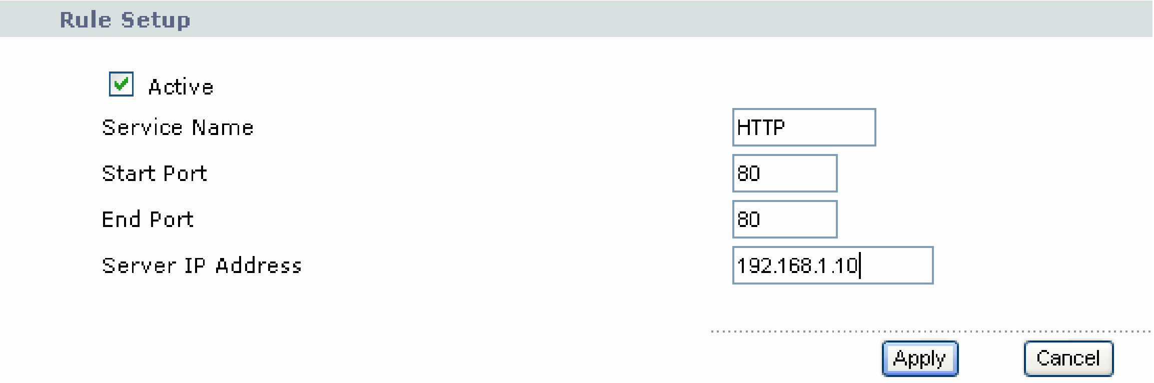
(1) Press the Edit icon to display the rule configuration screen.



#	Active	Name	Start Port	End Port	Server IP Address	Modify
1	💡		0	0		✎ 🗑
2	💡		0	0		✎ 🗑
3	💡		0	0		✎ 🗑
4	💡		0	0		✎ 🗑

(2) Active this rule and set the Service Name, Start Port, End Port and Service IP

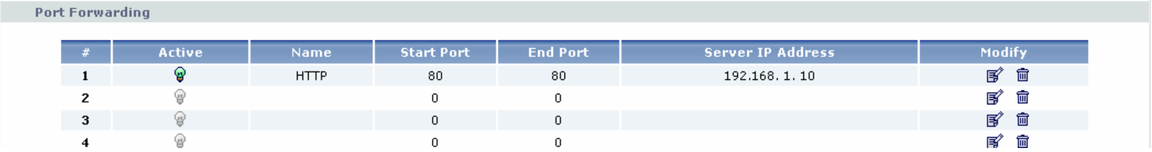
Address fields. Click Apply to save the settings.



Rule Setup

☑ Active	
Service Name	HTTP
Start Port	80
End Port	80
Server IP Address	192.168.1.10

(2) After you have successfully configured the rule, you can see the new rule in the Port Forwarding screen.



Port Forwarding

#	Active	Name	Start Port	End Port	Server IP Address	Modify
1	●	HTTP	80	80	192.168. 1. 10	✎ 🗑
2	○		0	0		✎ 🗑
3	○		0	0		✎ 🗑
4	○		0	0		✎ 🗑

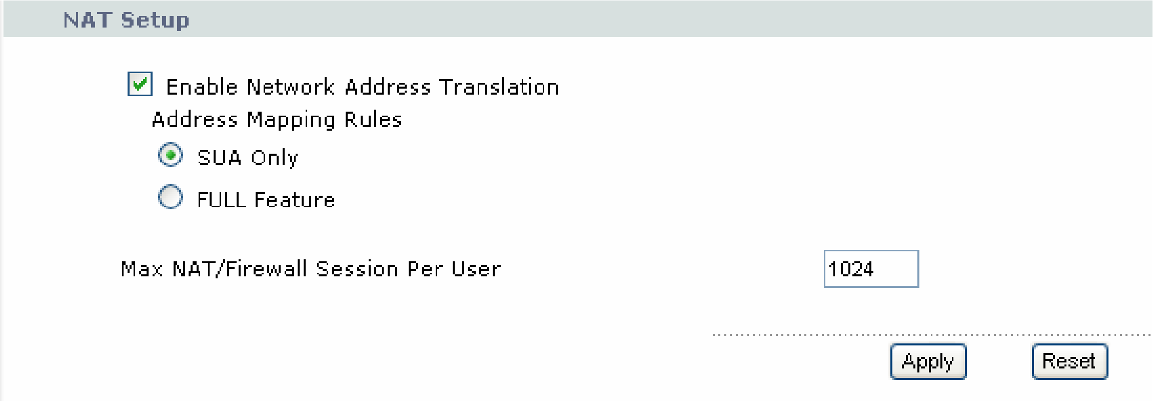
(3) If you want to change the rule, click Modify for the corresponding rule to display the edit screen.

The following table describes the port numbers for some common services

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

3. Using Full Feature NAT

To configure Full Feature NAT mode, click **Network > NAT > General** in the web configurator and select Full Feature in the NAT Option field.



NAT Setup

☑ Enable Network Address Translation

Address Mapping Rules

● SUA Only

○ FULL Feature

Max NAT/Firewall Session Per User: 1024

Configuring NAT

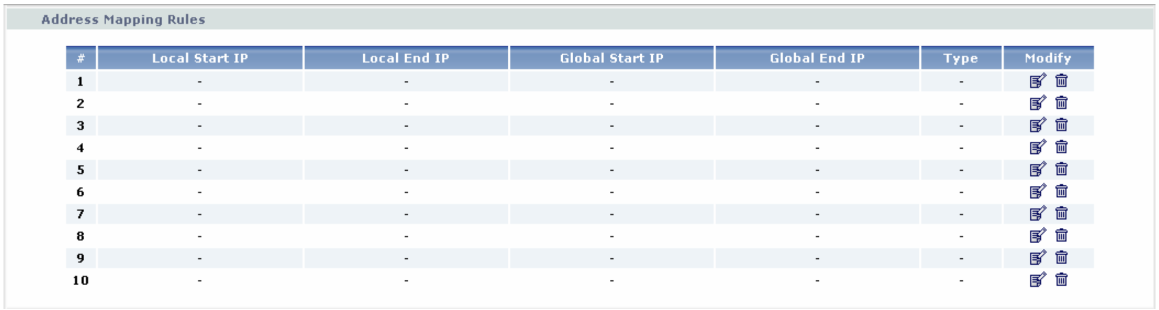
Address Mapping Sets and NAT Server Sets

The P-870HW-I 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.

The NAT Server Set is a list of LAN side servers mapped to external ports. You can configure the server set in the web configurator (click **Network > NAT > Port Forwarding**). To use the NAT server sets you have 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.

This section shows you how to configure address mapping sets using the web configurator.

First access the web configurator and click Advanced Setup > **Network > NAT > Address Mapping** to display the screen as shown.

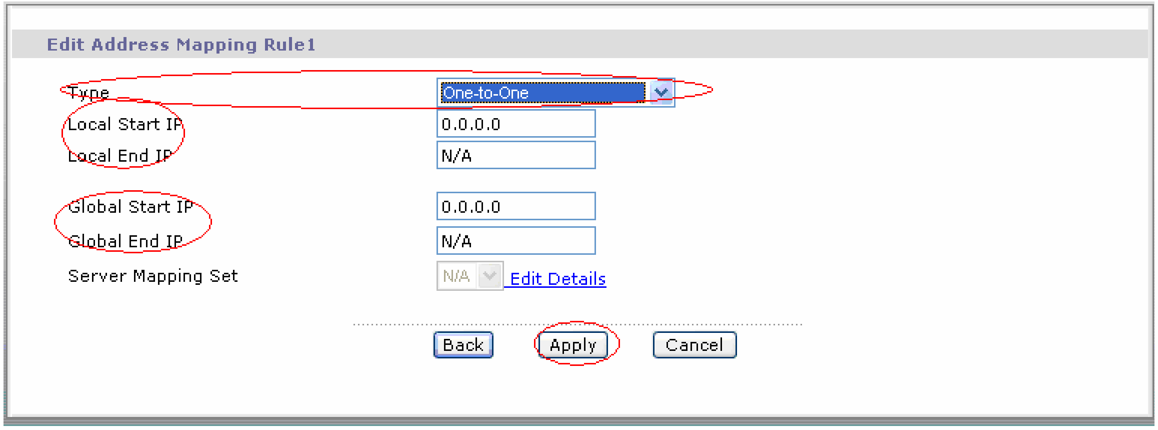


Address Mapping Rules

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

Click an Edit button to configure a server set. The following screen is for Address Mapping Set #1. You can configure up to 10 Address Mapping Rules for Set #1. You can edit or remove a rule by clicking the Edit or Delete button in the rule table.

Click the Edit button for rule #1 to display the configuration screen for the individual rule. Set the Mapping Type, Local and Global Start/End IP fields.



Edit Address Mapping Rule1

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

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 drop-down list box.	1. One-to-One 2. Many-to-One 3. Many-to-Many Overload 4. Many-One-to-One 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 set 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. That is you cannot have an End IP address beginning before the Start IP address.

NAT Server Sets

A NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu in older firmware versions). You can set inside servers for different services (such as 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 (for example, web service is on port 80 and FTP on port 21).

The following figure shows an example with a web server at 192.168.1.36 and a FTP server at 192.168.1.33. In this case, you need to specify port 80 for the web server at IP address 192.168.1.36 and port 21 for FTP server at IP address 192.168.1.33.

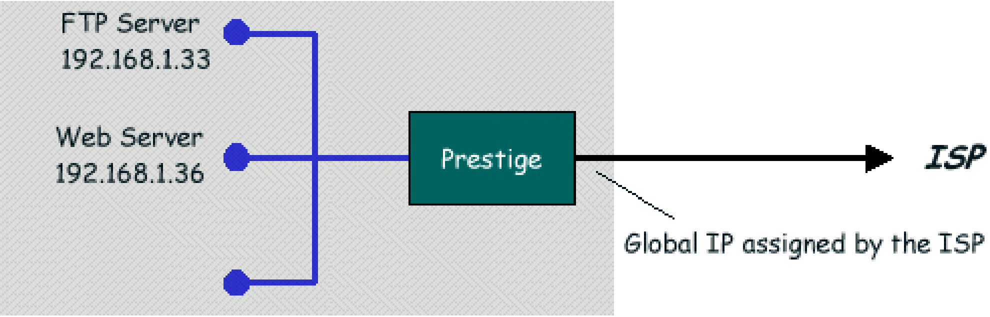


Figure: Configure Multiple Servers behind NAT

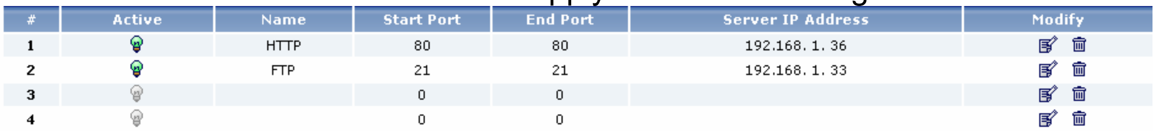
Please note that a server can support more than one service. For example, a server can provide both FTP and Mail services, while another server provides only web service.

The following procedure shows you how to configure a server behind NAT.

Step 1: Log into the web configurator and click **Network > NAT > Port Forwarding**.

Step 2: Click the Edit icon to rule 2 to display the configuration screen.

Step 3: Enable rule 2 and configure the Service Name, Start Port, End Port and Service IP Address fields. Then click Apply to save the changes.



#	Active	Name	Start Port	End Port	Server IP Address	Modify
1	●	HTTP	80	80	192.168. 1. 36	✎ 🗑
2	●	FTP	21	21	192.168. 1. 33	✎ 🗑
3	○		0	0		✎ 🗑
4	○		0	0		✎ 🗑

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

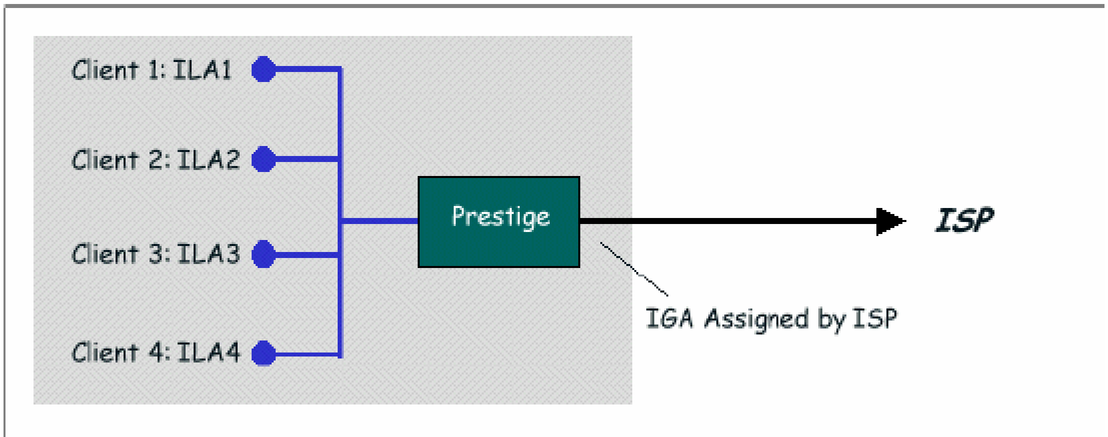
Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80

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

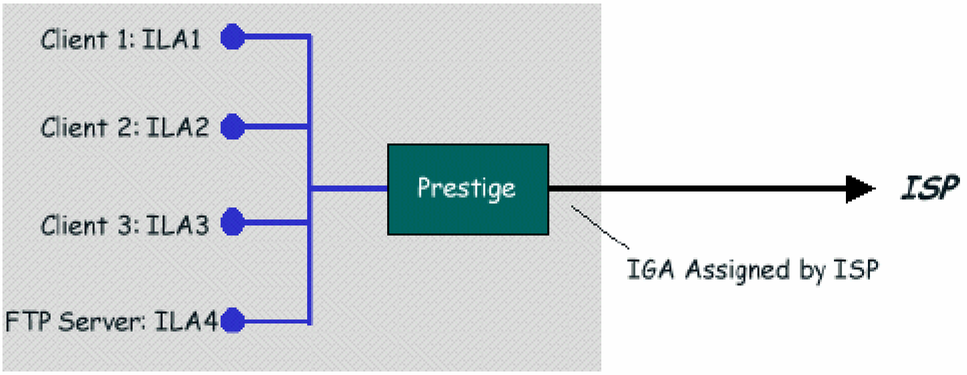
(1) Internet Access Only

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.



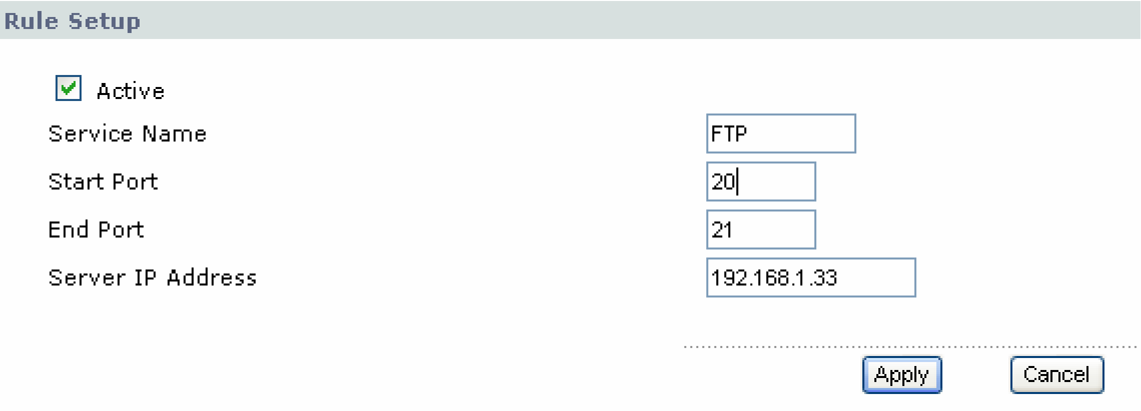
Internet Access Using NAT Many-to-One Mapping

(2) Internet Access with an Internal Server



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

In this case, configure the NAT network as shown in the network example (the pre-configured SUA Only set). Then **Network > NAT > Port Forwarding** to specify the Internet Server behind the NAT as shown below.

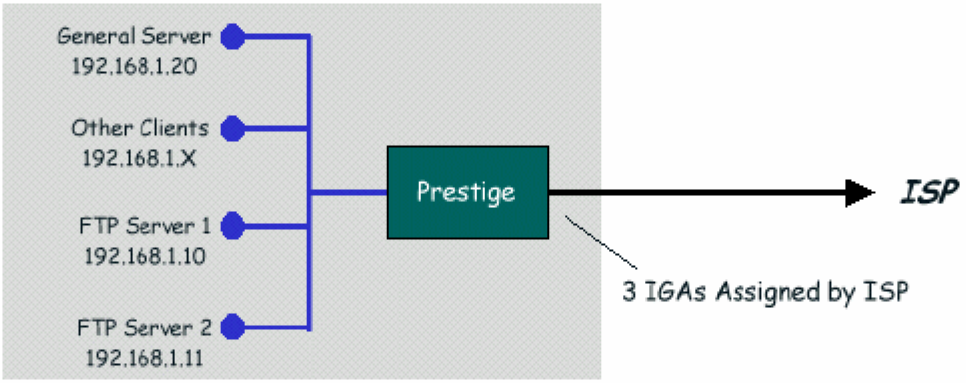


Rule Setup

☑ Active

Service Name	FTP
Start Port	20
End Port	21
Server IP Address	192.168.1.33

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

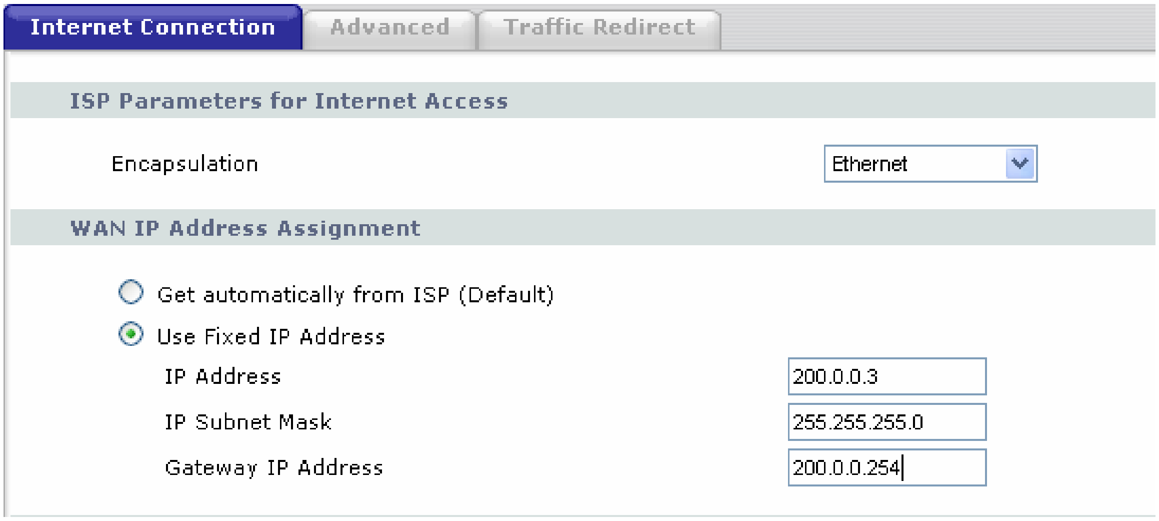


Mapping Multiple IGAs for clients and servers

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 web and mail services. 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 FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).
- Rule 2 (One-to-One type) to map FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).
- Rule 3 (Many-to-One type) to map 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. Select Full Feature in the NAT field and assign IGA3 as P-870HW-I's WAN IP Address.



ISP Parameters for Internet Access

Encapsulation: Ethernet

WAN IP Address Assignment

○ Get automatically from ISP (Default)

● Use Fixed IP Address

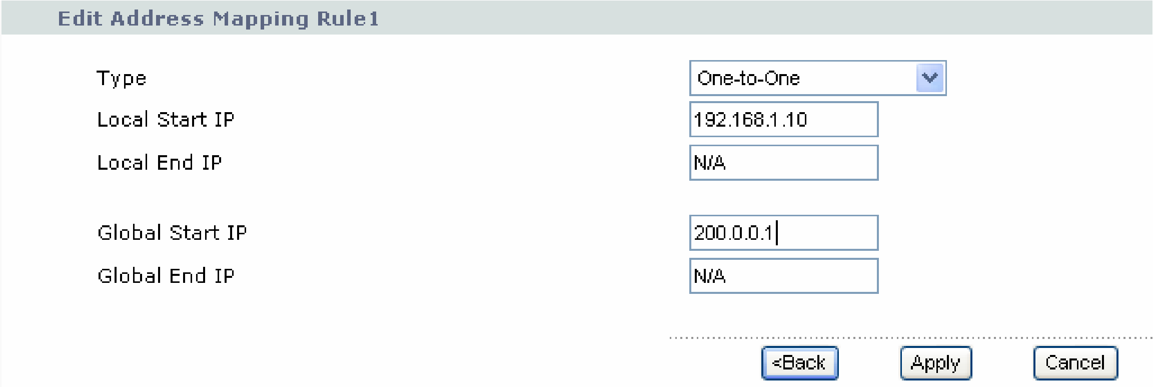
IP Address: 200.0.0.3

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 200.0.0.254

Step 2: In the web configurator, click Advanced Setup > **Network > NAT > Address Mapping** to configure Address Mapping Set #1. You can configure up to 10 rules in a set. The follow shows you how to configure the 4 rules for this example.

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


Edit Address Mapping Rule1

Type: One-to-One

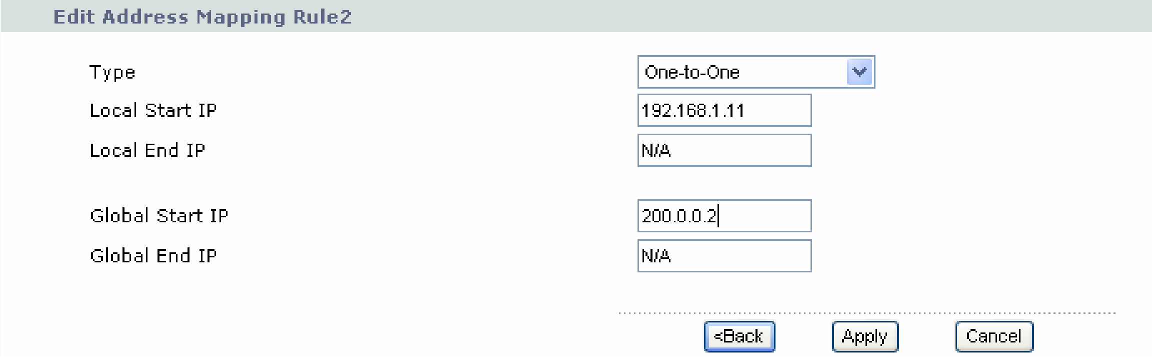
Local Start IP: 192.168.1.10

Local End IP: N/A

Global Start IP: 200.0.0.1

Global End IP: N/A

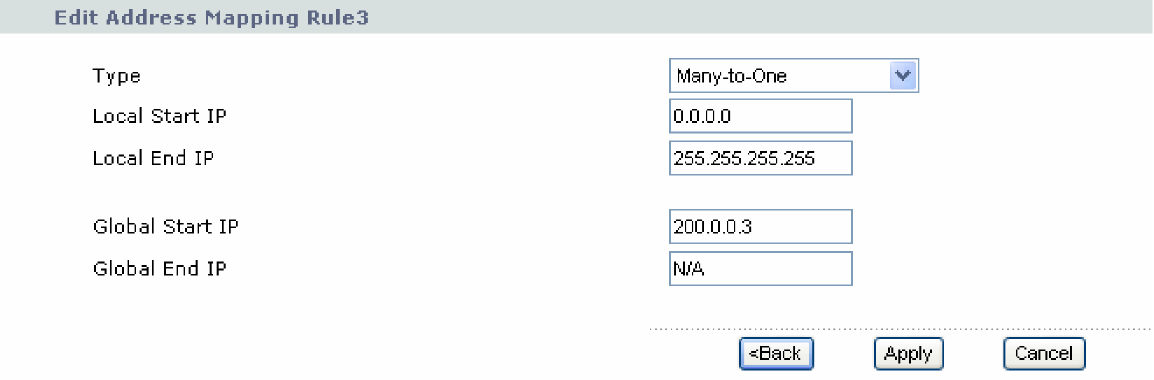
Rule 2 Setup: Selecting One-to-One type to map FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).



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

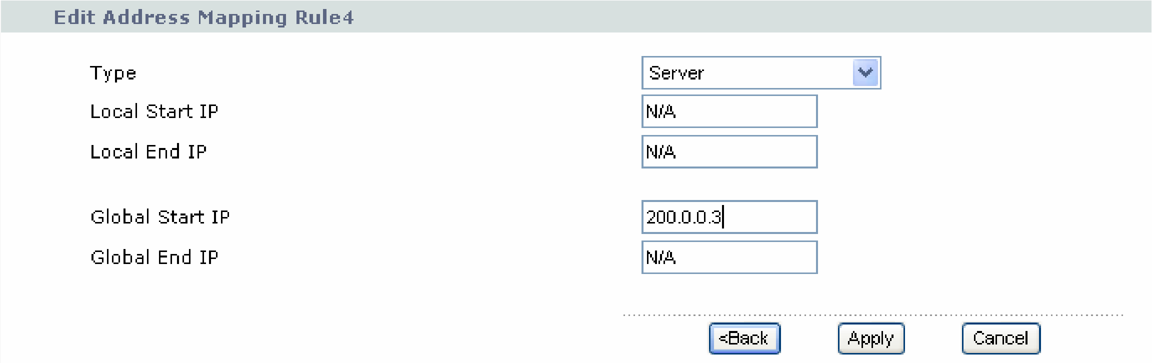
Rule 3 Setup: Select Many-to-One type to map other clients to IGA3 (200.0.0.3).



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

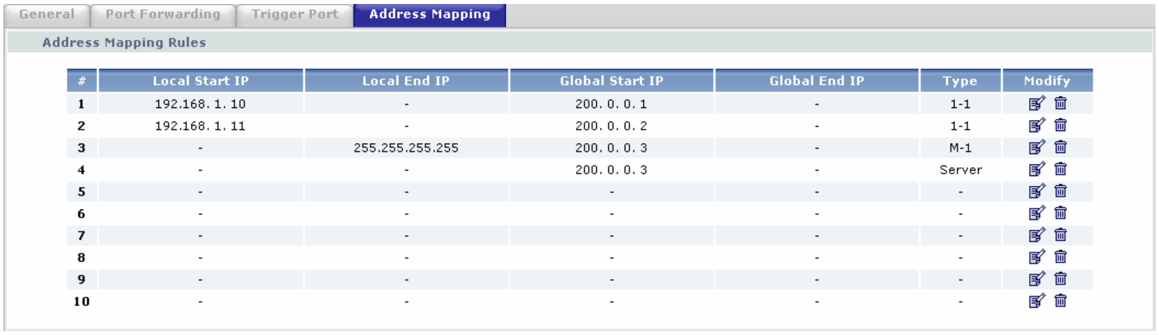
Rule 4 Setup: Select Server type to map the web and mail servers with ILA3 (192.168.1.20) to IGA3.



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

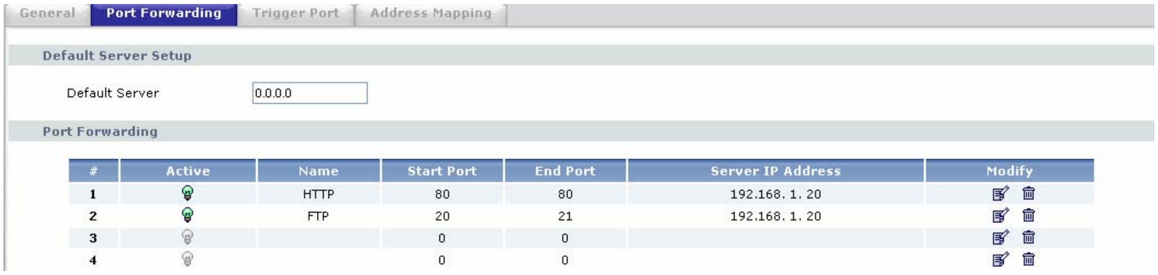
Check the rule setting in the Address Mapping Rules (click **Network > NAT-> Address Mapping**). The following shows an example.



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: Configure port forwarding rules for other incoming traffic to go to the internal web server and mail server. In the web configurator, click Advanced Setup > **Network > NAT > Port Forwarding**.



Default Server Setup

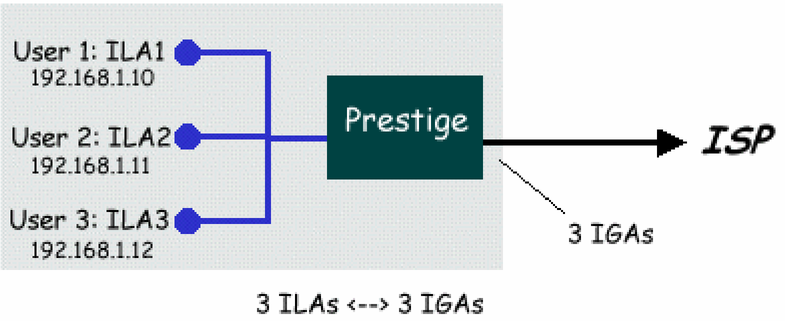
Default Server: 0.0.0.0

Port Forwarding

#	Active	Name	Start Port	End Port	Server IP Address	Modify
1	●	HTTP	80	80	192.168. 1. 20	✎ 🗑
2	●	FTP	20	21	192.168. 1. 20	✎ 🗑
3	○		0	0		✎ 🗑
4	○		0	0		✎ 🗑

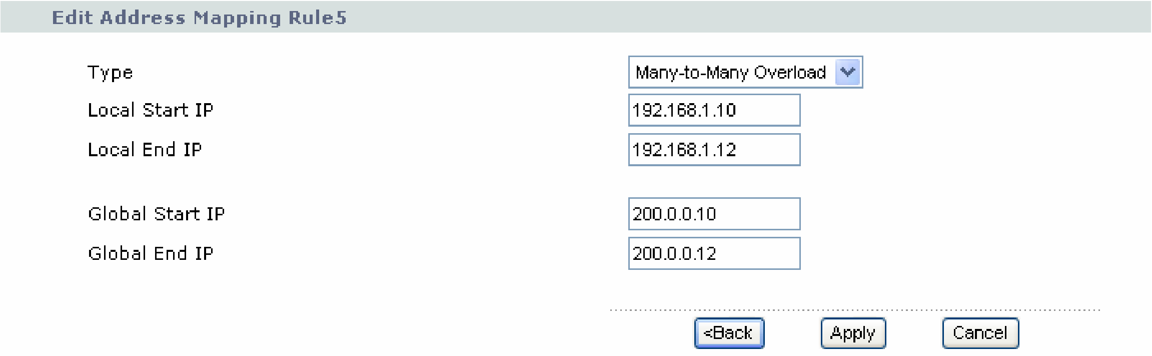
(4) Non NAT Friendly Application Support

Some servers providing Internet applications, such as some mIRC servers, do not allow multiple users to log in using the same IP address. In this case, use Many-to-Many No Overload or One-to-One NAT mapping types to allow each user to log into 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

The following figure shows the settings of a Many-to-Many No Overload mapping rule.



Edit Address Mapping Rule5

Type	Many-to-Many Overload
Local Start IP	192.168.1.10
Local End IP	192.168.1.12
Global Start IP	200.0.0.10
Global End IP	200.0.0.12

Similarly, configure the other three One-to-One mapping rules.

4. Using Dynamic DNS (DDNS)

- What is DDNS?

DDNS service is an IP Registry providing 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 address associated with dynamic IP addresses.

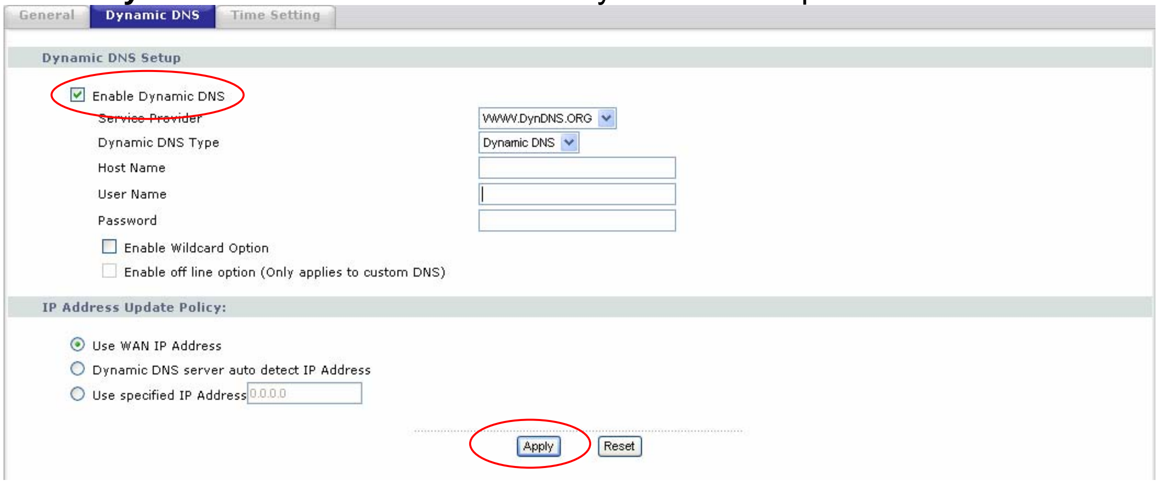
Without DDNS, we always have to tell users to use the WAN IP address of the P-870HW-I to access the internal server. This is inconvenient for users if this IP address is dynamic. With DDNS support on the P-870HW-I, you can assign a DNS name (e.g., www.zyxel.com.tw) to your server (e.g., Web server) from a DDNS server. Therefore outside users can always access the web server using the name “www.zyxel.com.tw” regardless of the WAN IP address of the P-870HW-I.

When the ISP assigns the P-870HW-I a new WAN IP address, the P-870HW-I must inform the DDNS server the change of this IP address so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

The DDNS server the P-870HW-I supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

- Setup the DDNS

1. Before configuring DDNS settings on the P-870HW-I, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you are given a hostname for your internal server and a password used to update the IP-to-DDNS entry on the DDNS server.
2. Log into the web configurator and click Advanced Setup > **Maintenance > Dynamic DNS**. Select the Active Dynamic DNS option to enable DDNS.



Dynamic DNS Setup

☑ Enable Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Dynamic DNS Type: Dynamic DNS

Host Name:

User Name:

Password:

□ Enable Wildcard Option

□ Enable off line option (Only applies to custom DNS)

IP Address Update Policy:

● Use WAN IP Address

○ Dynamic DNS server auto detect IP Address

○ Use specified IP Address 0.0.0.0

Key Settings:

Option	Description
Service Provider	Enter the DDNS server in this field. Currently, we support WWW.DYNDNS.ORG.
Host Name	Enter the hostname you subscribe from the 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 WWW.DYNDNS.ORG supports. Note that the Wildcard option is available only when the provider is http://www.dyndns.org/.

5. Network Management Using SNMP

- ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some P-870HW-I routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. Further, you can also add ZyXEL private MIBs in the NMS to monitor and control additional system variables. 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 any 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 IDSL or WAN link 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 IDSL or WAN link 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 a 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.

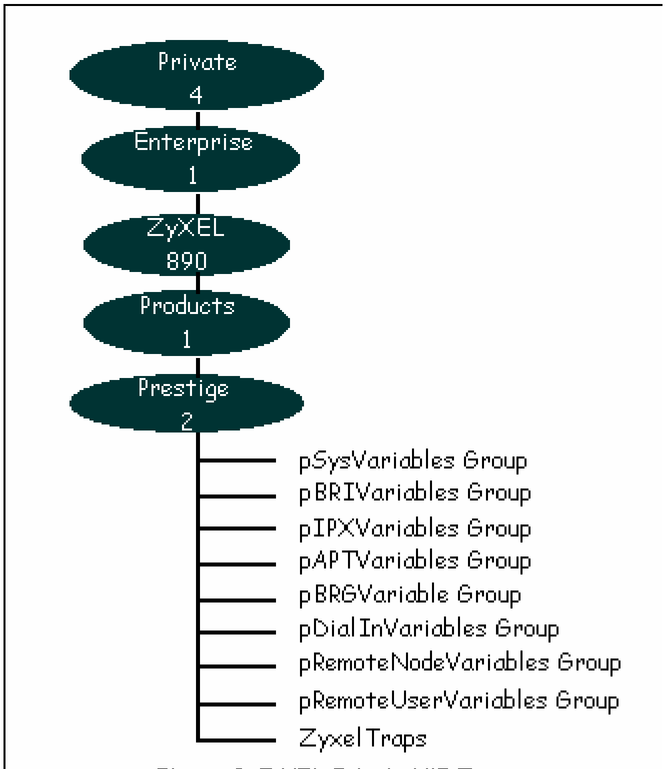
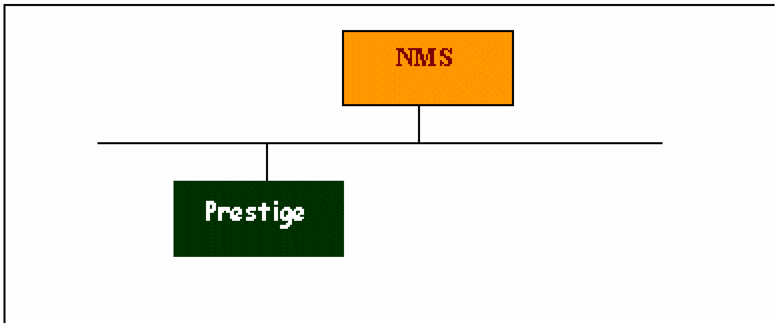
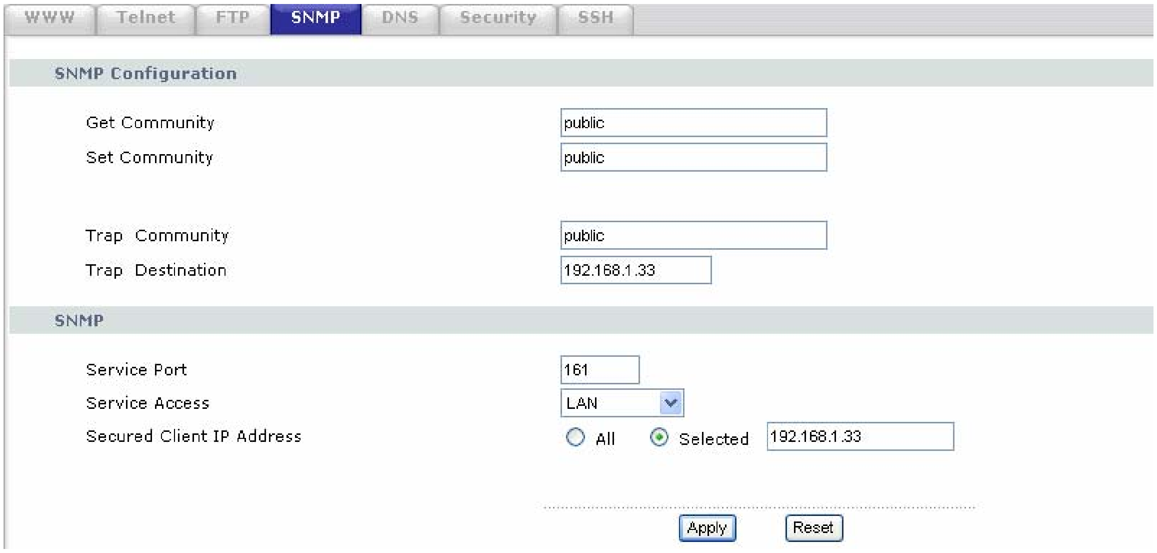


Figure 3: ZyXEL Private MIB Tree

- Download ZyXEL private MIBs
- Configure the P-870HW-I for SNMP



You can configure SNMP related settings on the P-870HW-I in the web configurator. Click Advanced Setup > **Management > Remote MGNT > SNMP**.



SNMP Configuration

Get Community: public

Set Community: public

Trap Community: public

Trap Destination: 192.168.1.33

SNMP

Service Port: 161

Service Access: LAN

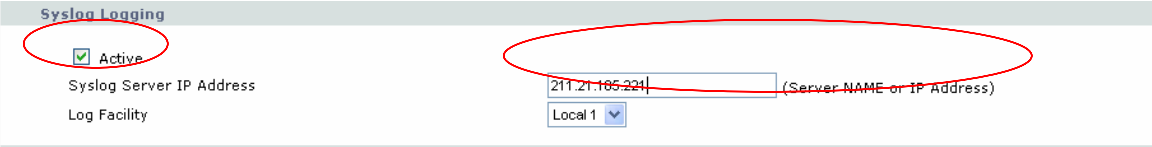
Secured Client IP Address: ○ All ● Selected 192.168.1.33

Key Settings:

Option	Descriptions
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
Trap Community	Enter the community name in each sent trap to the NMS. This Trap Community must match what the NMS is expecting. The default is 'public'.
Trap Destination	Enter the IP address of the NMS that you wish to send the traps to. If 0.0.0.0 is entered, the P-870HW-I will not send trap any NMS manager.

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

6. Using syslog



Syslog Logging

☑ Active

Syslog Server IP Address: 211.21.105.221 (Server NAME or IP Address)

Log Facility: Local 1

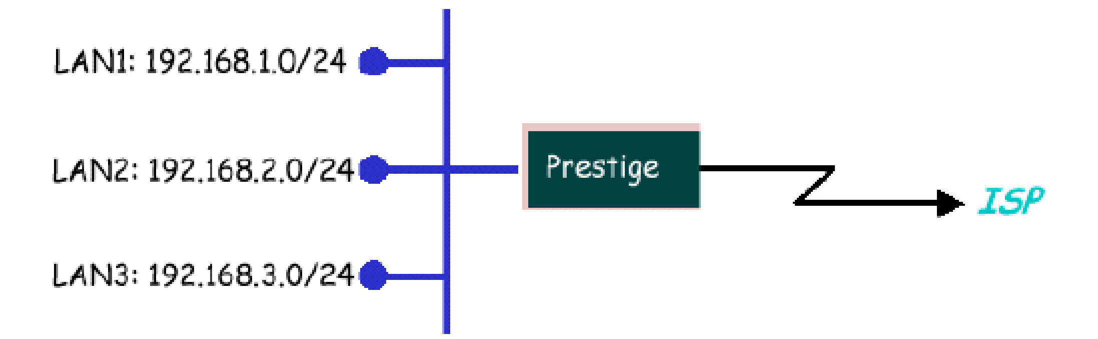
You can configure syslog settings in the web configurator. Click Advanced Setup > **Maintenance > Logs > Log Settings > Syslog logging**.

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

7. Using IP Alias

- What is IP Alias?

In a typical environment, a LAN router is required to connect two local networks. The P-870HW-I can connect three local networks to an ISP or a remote node. This feature is known 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-870HW-I's single user account. See the figure below.

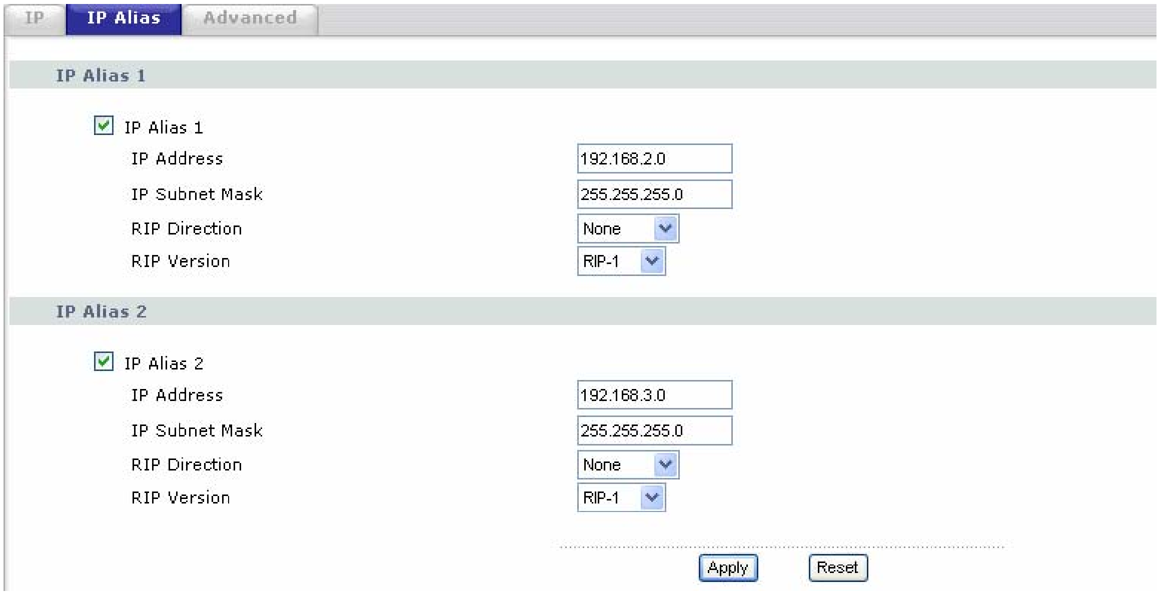


The Prestige's IP Alias connects three local networks to the Internet

The P-870HW-I supports three virtual LAN interfaces via its single physical Ethernet interface. You can configure the first network in the web configurator. Click Advanced Setup > **Network > DHCP Server**. Configure the second and third networks (IP Alias 1 and IP Alias 2) by clicking **Network > LAN > IP Alias**.

There are three internal virtual LAN interfaces for the P-870HW-I to route packets from/to the three networks correctly. They are enif0 for the main network, enif0:0 for IP alias 1 and enif0:1 for IP alias 2. Therefore, three routes are created in the P-870HW-I as shown below when the three networks are configured. If the P-870HW-I's DHCP is also enabled, the IP pool for the clients can be any of the three networks.

- IP Alias Setup



IP Alias 1

☑ IP Alias 1

IP Address: 192.168.2.0

IP Subnet Mask: 255.255.255.0

RIP Direction: None

RIP Version: RIP-1

IP Alias 2

☑ IP Alias 2

IP Address: 192.168.3.0

IP Subnet Mask: 255.255.255.0

RIP Direction: None

RIP Version: RIP-1

(1) Edit the first network in the web configurator by clicking Advanced Setup> **Network > DHCP Server Setup**. Use this screen to configure the IP address of the first network on the P-870HW-I.

Key Settings:

DHCP Setup	If the P-870HW-I'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-870HW-I. This will create the first route on the enif0 interface.

(2) Edit the second and third networks by clicking **Network > LAN > IP Alias**. Then configure the IP addresses for the second and third networks on the P-870HW-I.

Key Settings:

IP Alias 1	Select to enable the second network and enter the second LAN IP address This will create the second route on the enif0:0 interface.
IP Alias 2	Select to enable the third network and enter the third LAN IP address. This will create the third route on the enif0:1 interface.

8. 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-870HW-I queries all directly connected networks to gather group membership information.

After that, the P-870HW-I updates the information by periodic queries. The P-870HW-I’s implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on the Ethernet interface or for the remote nodes.

- IP Multicast Setup

(1) Enable IGMP in P-870HW-I's LAN. In the web configurator click Advanced Setup > **Network > WAN > Advanced > RIP > Multicast Setup** to display the configuration screen.

Key Settings:

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

9. Using Bandwidth Management

- Why Bandwidth Management (BWM)?

There are many different traffic types for Internet applications. Some traffic may require high bandwidth, such as FTP (File Transfer Protocol). Others (such as VoIP traffic) may not require high bandwidth, but they require a stable supply of bandwidth for smooth operation. VoIP quality deteriorates if all of the outgoing bandwidth is hogged by other applications. In addition, chances are that you would like to grant higher bandwidth for a user with a specific IP address in your network. These are some of the main reasons why we need bandwidth management.

- Using BWM

Step 1: In the web configurator, click Advanced Setup > **Management > Bandwidth MGMT> Configuration** and activate bandwidth management on the interface you would like to manage. In this example, we enable the BWM function on the WAN interface.
Enter the total speed for this interface that you want to allocate using bandwidth

management. This appears as the bandwidth budget of the interface’s root class. Select how you want the bandwidth to be allocated. Priority-Based means bandwidth is allocated based on the priority level, so traffic with the highest priority would be served first, then the second priority is served and so on. If you select Fairness-Based, then bandwidth is allocated by ratio. Which means that if class A needs 300 kbps, class B needs 600 kbps, then the ratio of A and B's actual bandwidth is 1:2. Thus we need 450 kbps of bandwidth in total and assign 150 kbps and 300 kbps to classes A and B respectively. We select Priority-Based in this example.

Key Settings:

Active	Select this option to enable BWM on the interface. Note that if you want to manage traffic from WAN to LAN, you need to enable BWM on the LAN interface. If you want to management traffic from WAN to DMZ, then enable BWM on the DMZ interface.
Speed	Enter the total speed to manage on this interface. This value is the budget of the class tree's root.
Scheduler	Choose the method to allocate bandwidth on this interface. Priority-Based allocates bandwidth based on the priority level while the Fairness-Based method allocates bandwidth by ratio.
Maximize Bandwidth Usage	Select this option if you want to give the remaining bandwidth on the interface to the classes who need more bandwidth than the configured amount. Clear this check box if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the bandwidth of each class at the configured value. Note that to meet the second condition, you must also disable Use All Managed Bandwidth for the BWM rule.

Step 2: In the web configurator, click Advanced Setup > **Management > Bandwidth MGMT > Configuration** and set the interface, Service, Priority, and Allocated Bandwidth settings for this rule. Click Apply to save the configuration.

Step 3: You can change the rule settings by clicking the Edit button for the rule.
Key Settings:

Rule Name	Enter a descriptive name to identify this rule. For example, 'WWW'
BW Budget	Specify the bandwidth to allocate to this rule
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Use All Managed Bandwidth	Select this option if you want to allow this class to borrow bandwidth from its parents when the required bandwidth is higher than the configured amount. Clear this checkbox if you want to limit the bandwidth of this class at the configured value.(Note that you must also disable Maximize Bandwidth Usage on the interface to meet the condition.)
Service	Select User-defined, SIP, FTP, or H.323 to specify the traffic types
Destination IP Address	Enter the IP address of destination that for this class.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the destination port number of the traffic.
Source IP Address	Enter the IP address of source for this class. Since BWM is done before NAT, you must use the original IP address (before NAT translation) for the ‘LAN to WAN’ traffic.
Source Subnet Mask	Enter the destination subnet mask.
Source Port	Enter the source port number of the traffic.
Protocol ID	Enter the protocol number of the traffic. 1 for ICMP, 6 for TCP or 17 for UDP

After configuring BWM, you can check the current bandwidth of the configured traffic by clicking Advanced Setup > **Management > Bandwidth MGMT > Monitor**.

10 Using Bandwidth Management

Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only. All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has obtained the UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

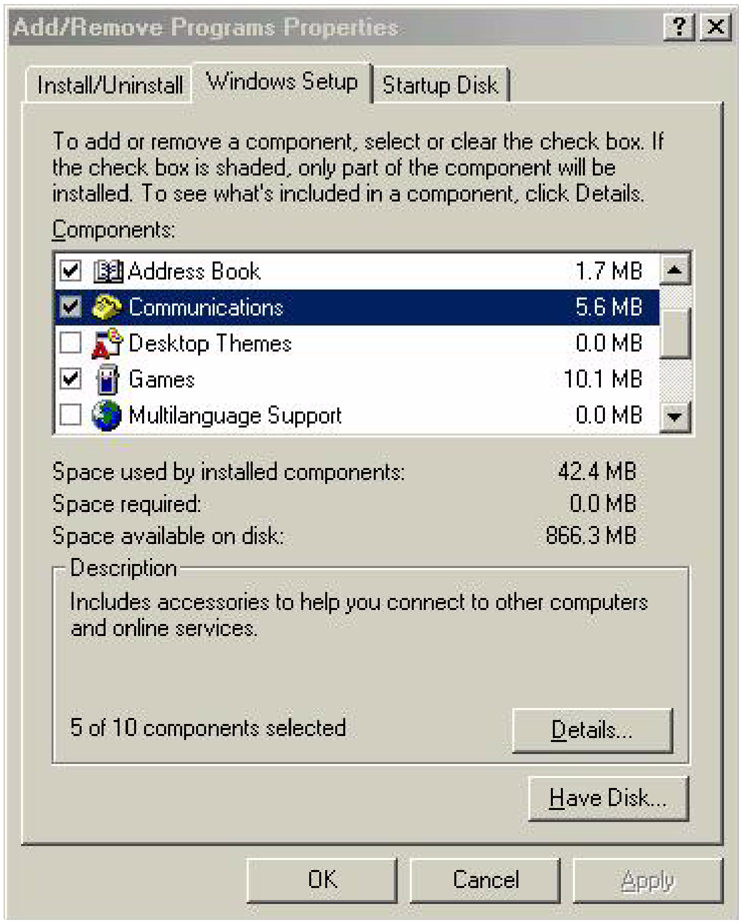
Installing UPnP in Windows Example

This section shows you how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



Add/Remove Programs Properties

To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

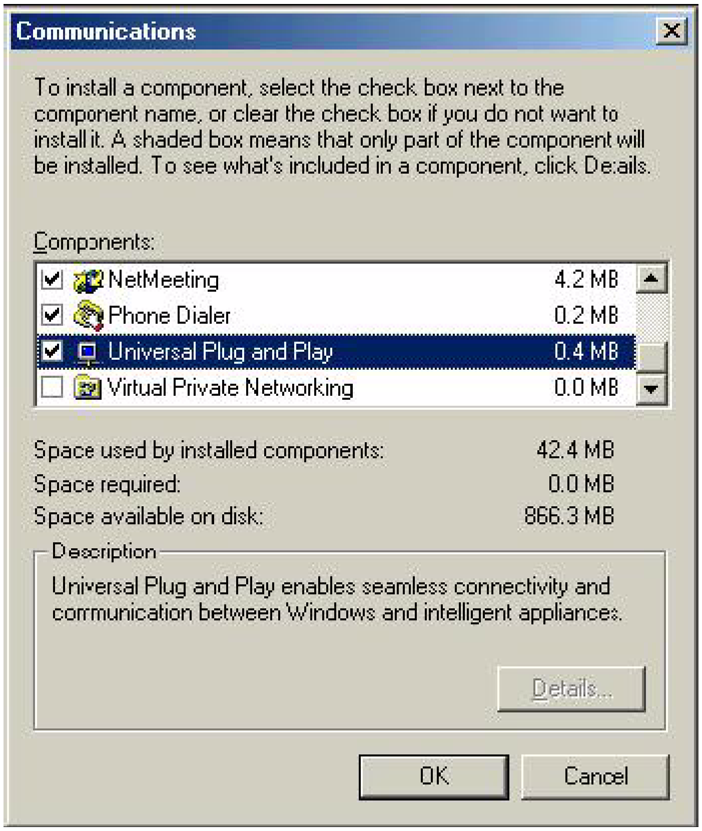
Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

Figure: Add/Remove Programs: Windows Setup: Communication

3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.



Communications

To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
□	Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

Figure Add/Remove Programs: Windows Setup: Communication: Components

4. Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
5. Restart the computer when prompted.

Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.
1. Click **Start** and **Control Panel**.
2. Double-click **Network Connections**.
3. In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

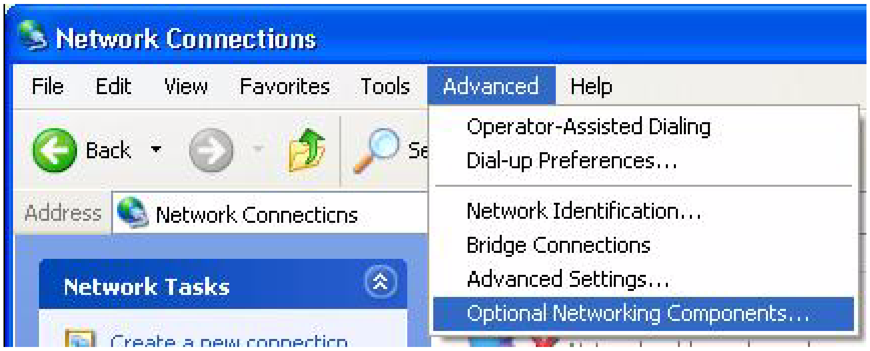
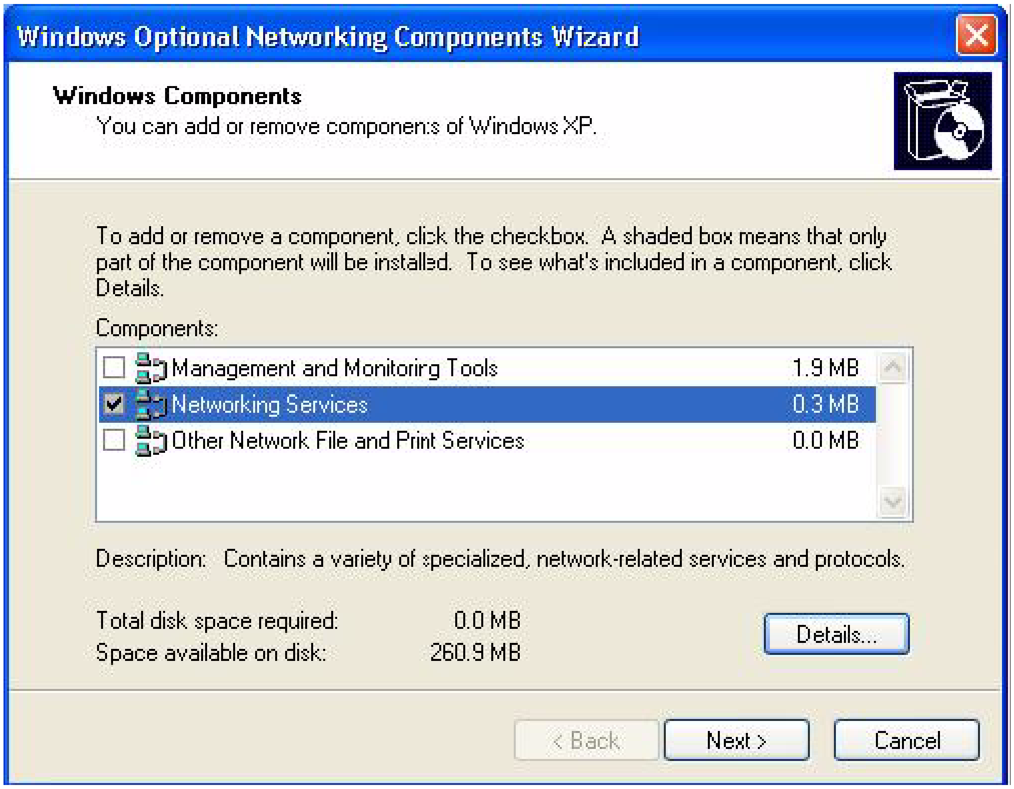


Figure Network Connections

4. The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.



Windows Optional Networking Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

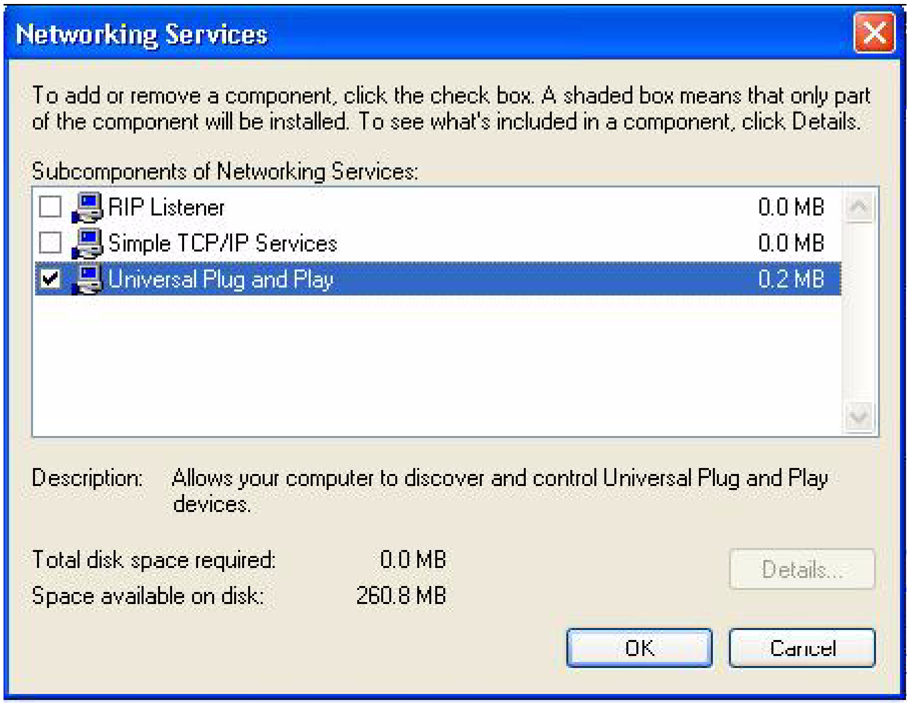
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

Figure Windows Optional Networking Components Wizard

5. In the **Networking Services** window, select the **Universal Plug and Play** check box.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

- □ RIP Listener 0.0 MB
- □ Simple TCP/IP Services 0.0 MB
- ☑ Universal Plug and Play 0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB
Space available on disk: 260.8 MB

Figure Networking Services

6. Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.
Make sure the computer is connected to a LAN port on the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device
1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
2. Right-click the icon and select **Properties**.

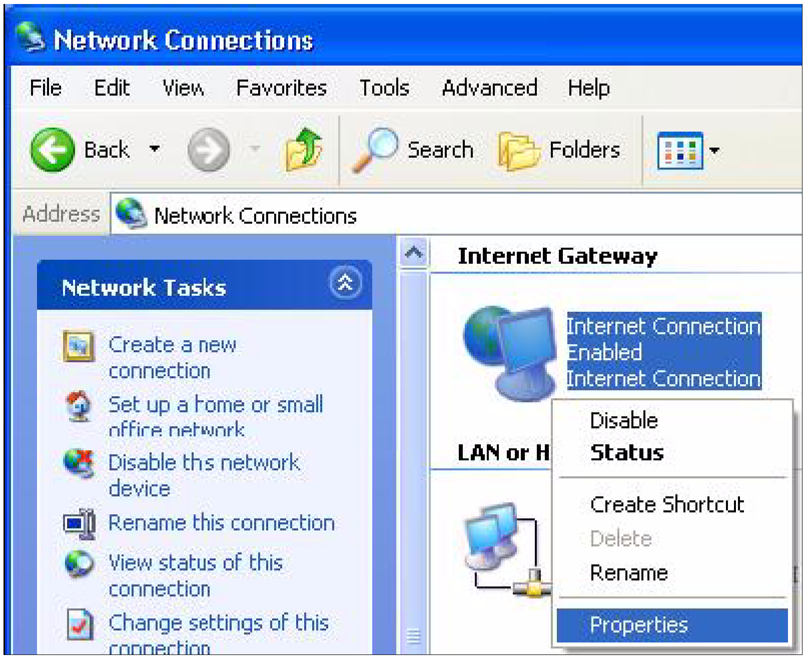
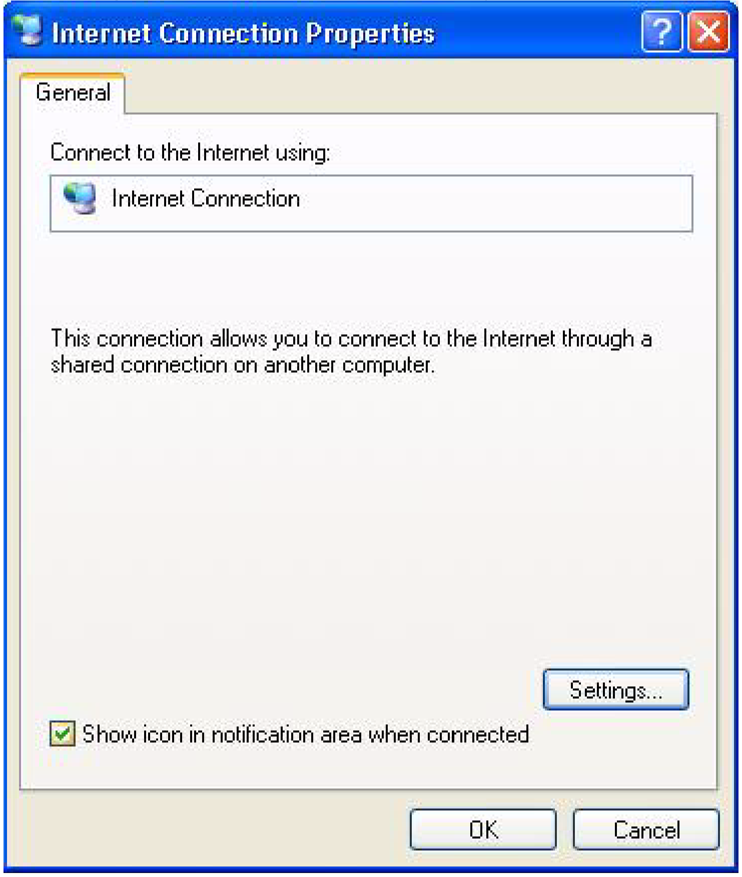


Figure Network Connections

3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.



Connect to the Internet using:

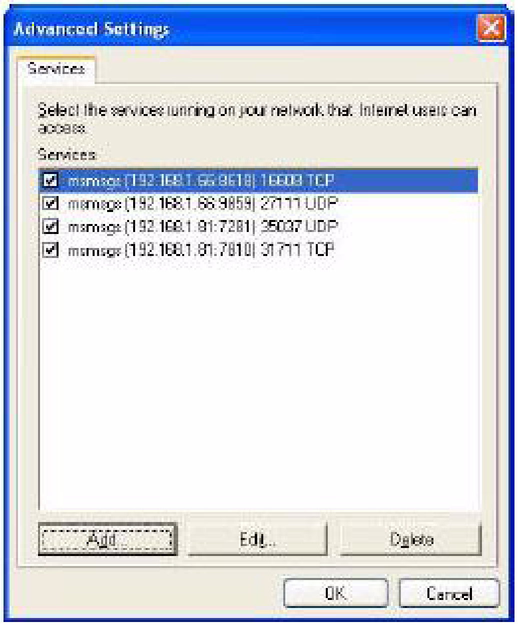
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

Figure Internet Connection Properties

4. You may edit or delete the port mappings or click **Add** to manually add port mappings.



Advanced Settings

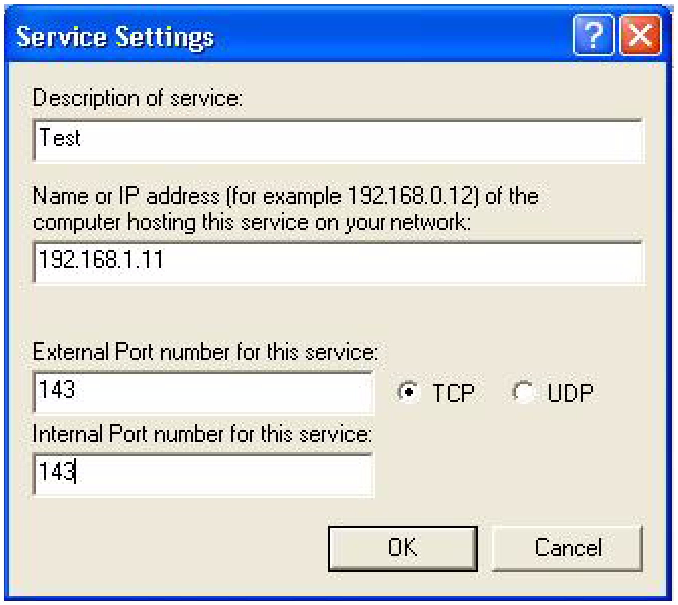
Services

Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:9618) 16603 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure Internet Connection Properties: Advanced Settings



Service Settings

Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

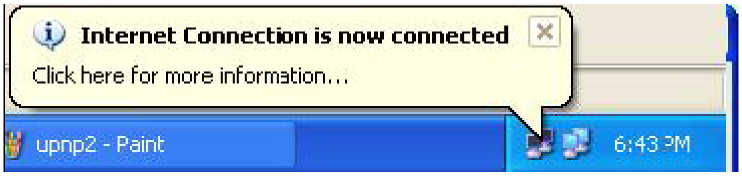
External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

Figure Internet Connection Properties: Advanced Settings: Add

5. When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6. Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

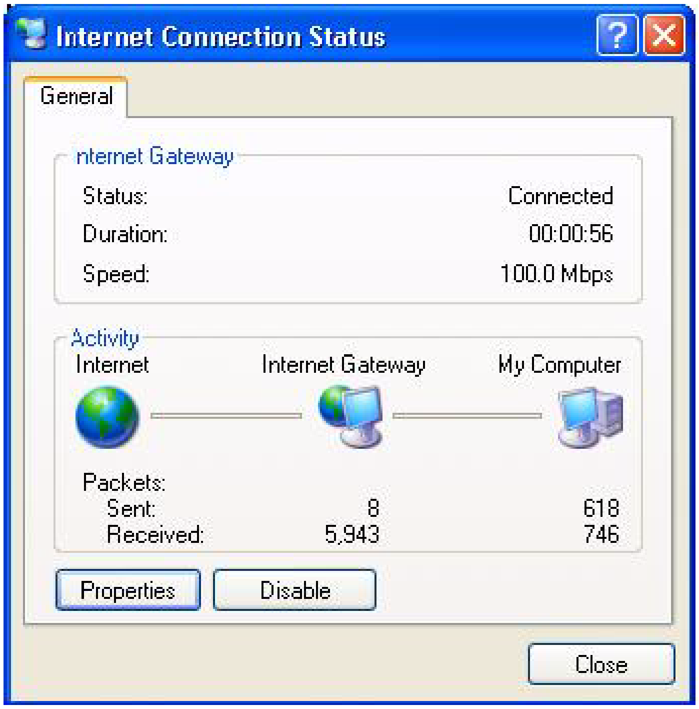


Internet Connection is now connected

Click here for more information...

Figure 134 System Tray Icon

7. Double-click on the icon to display your current Internet connection status.



Internet Connection Status

General

nternet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		8	618
Received:		5,943	746

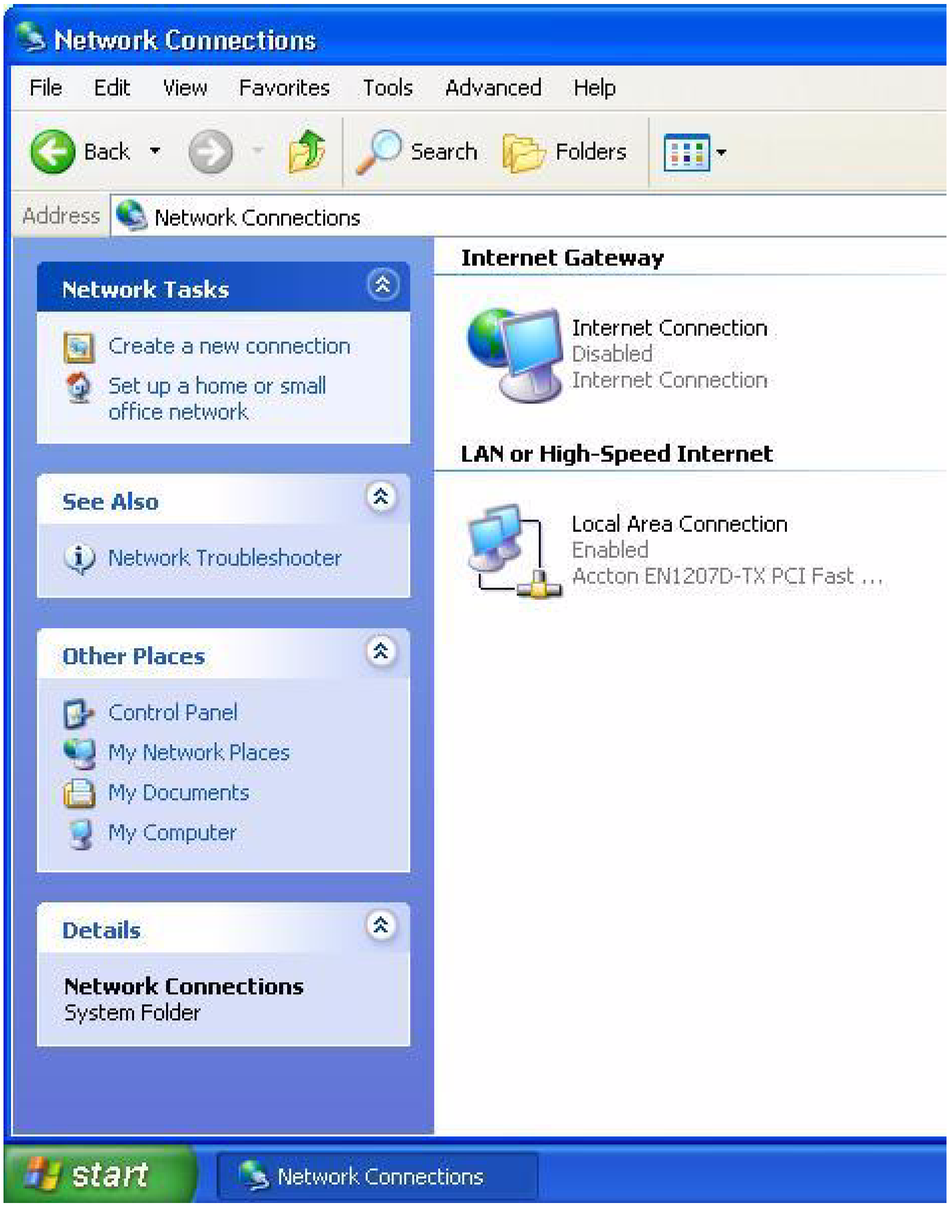
Figure Internet Connection Status

Easy Web Configurator Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

1. Click **Start** and then **Control Panel**.
2. Double-click **Network Connections**.
3. Select **My Network Places** under **Other Places**.



Network Connections
System Folder

Internet Gateway

Internet Connection
Disabled
Internet Connection

LAN or High-Speed Internet

Local Area Connection
Enabled
Accton EN1207D-TX PCI Fast ...

Figure Network Connections

4**.** An icon with the description for each UPnP-enabled device displays under **Local Network**.
5. Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

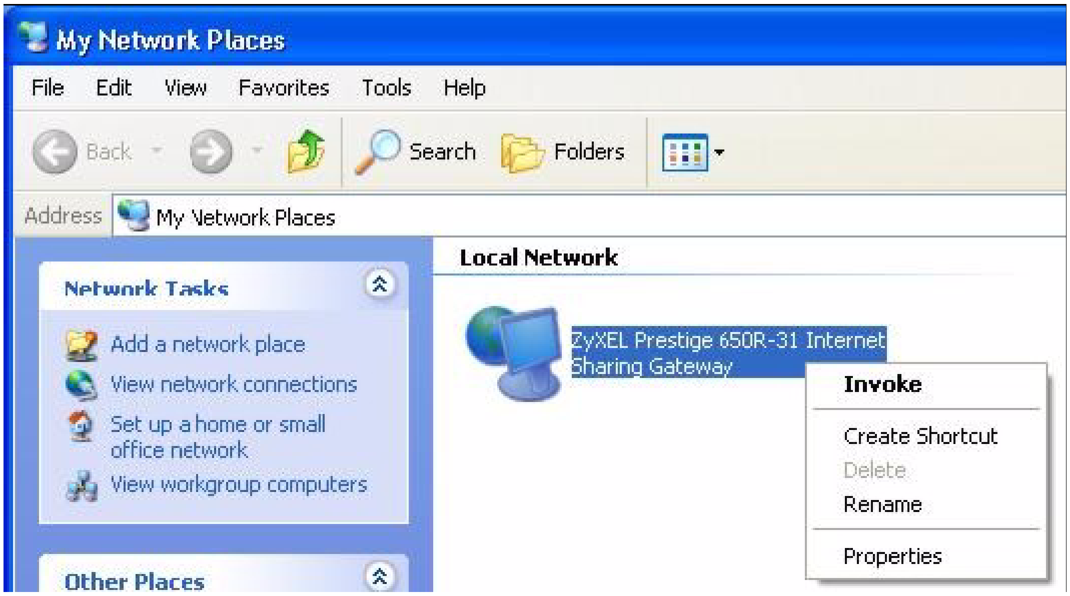
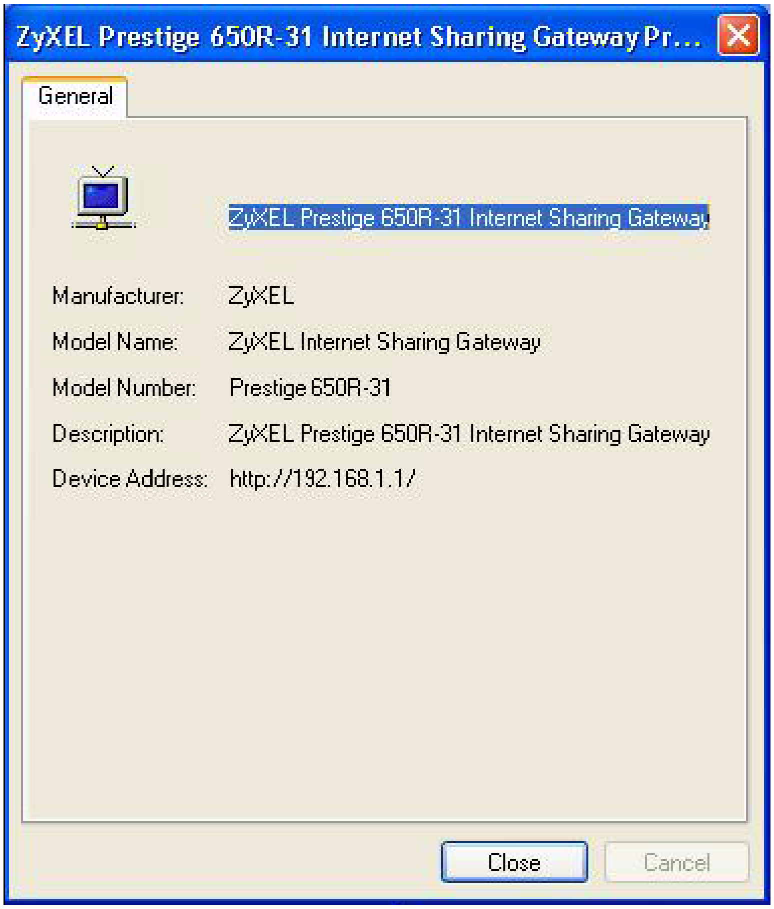


Figure Network Connections: My Network Places

6. Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.



ZyXEL Prestige 650R-31 Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: Prestige 650R-31

Description: ZyXEL Prestige 650R-31 Internet Sharing Gateway

Device Address: http://192.168.1.1/

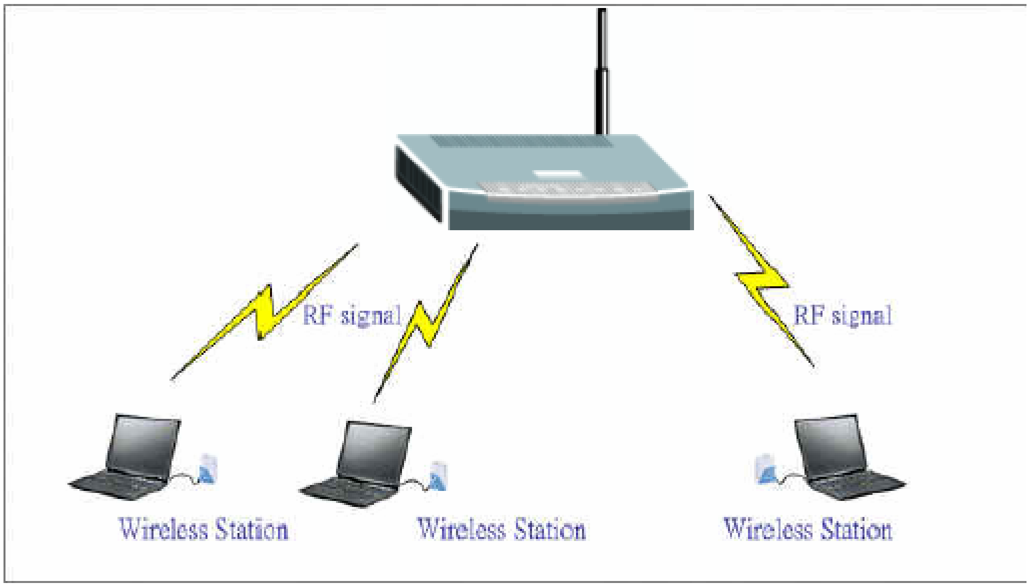
Figure Network Connections: My Network Places: Properties: Example

Wireless Application Notes

1. Configuring Infrastructure mode

Infrastructure Introduction

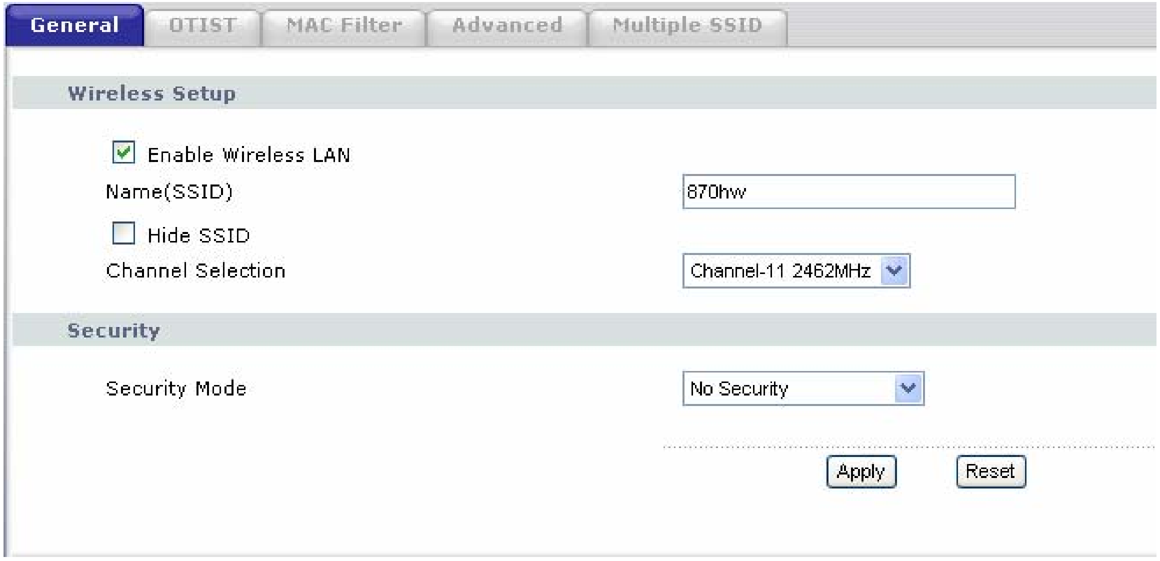
In Infrastructure WLANs, network resources are shared via employing multiple Access Points (APs) that are both connecting WLAN to the wired network and transfer the wireless network traffic in the very neighborhood.



Configure Wireless Access Point to Infrastructure mode using Web configurator.

To configure Infrastructure mode of your P-870HW-I wireless AP, please follow the steps below.

Step 1: Login Web Configurator, Advanced Setup, **Network -> Wireless LAN -> General**. Configure the basic parameters for the Wireless LAN.



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): 870hw

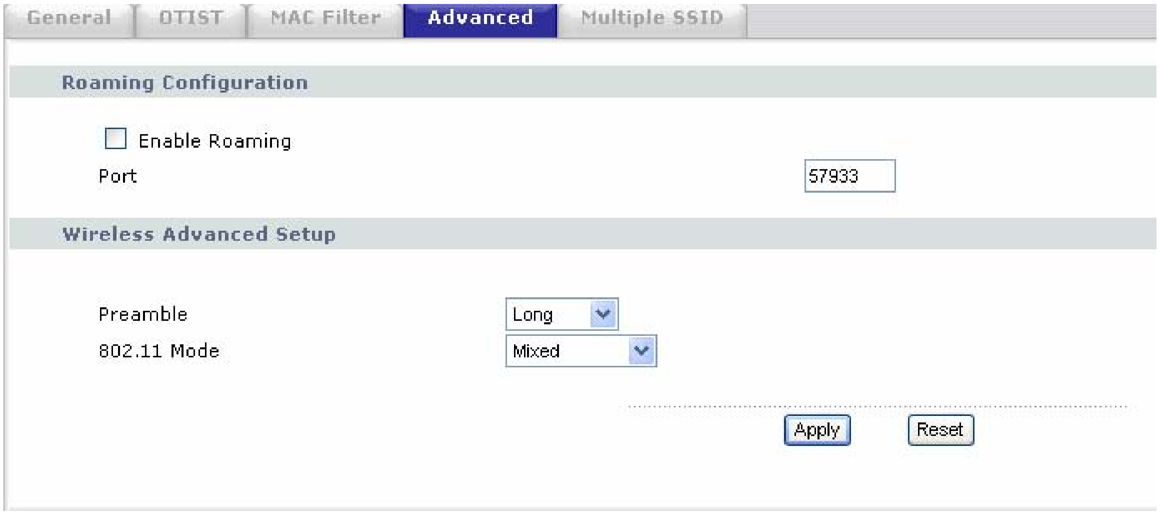
□ Hide SSID

Channel Selection: Channel-11 2462MHz

Security

Security Mode: No Security

Step 2: If you want to configure more detailed settings, click the ‘Advanced’ tag:



Roaming Configuration

□ Enable Roaming

Port: 57933

Wireless Advanced Setup

Preamble: Long

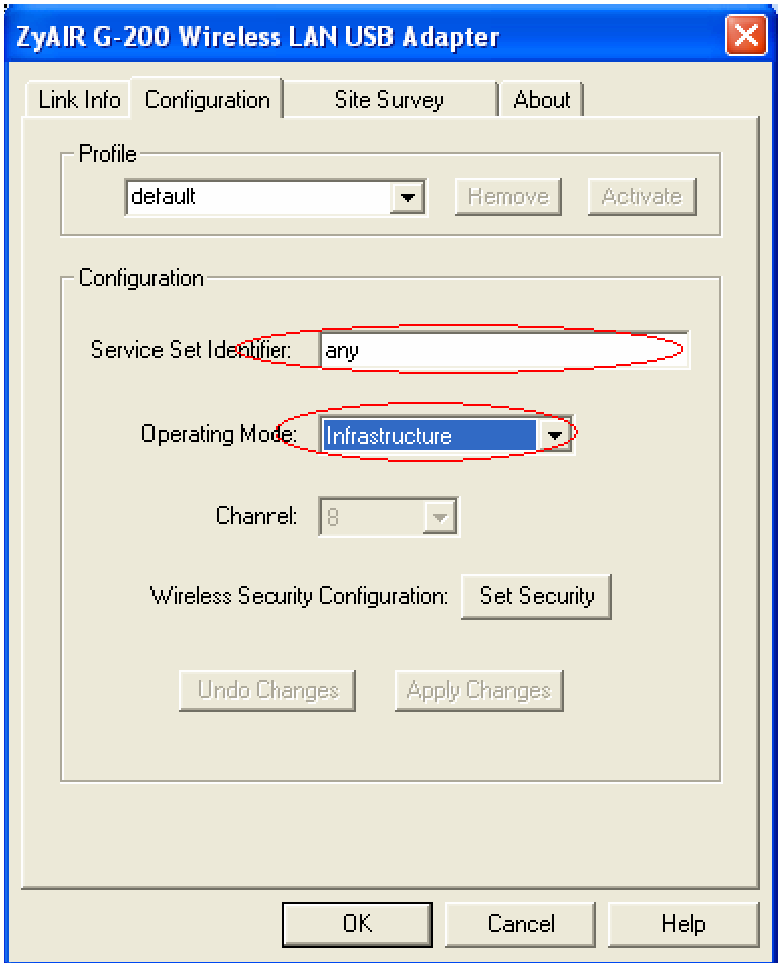
802.11 Mode: Mixed

Configuration Wireless Station to Infrastructure mode

To configure Infrastructure mode on your ZyAIR G-200 Wireless Network Adapter, please follow these steps:

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

Step 2: Select configuration tab.



ZyAIR G-200 Wireless LAN USB Adapter

Profile: default

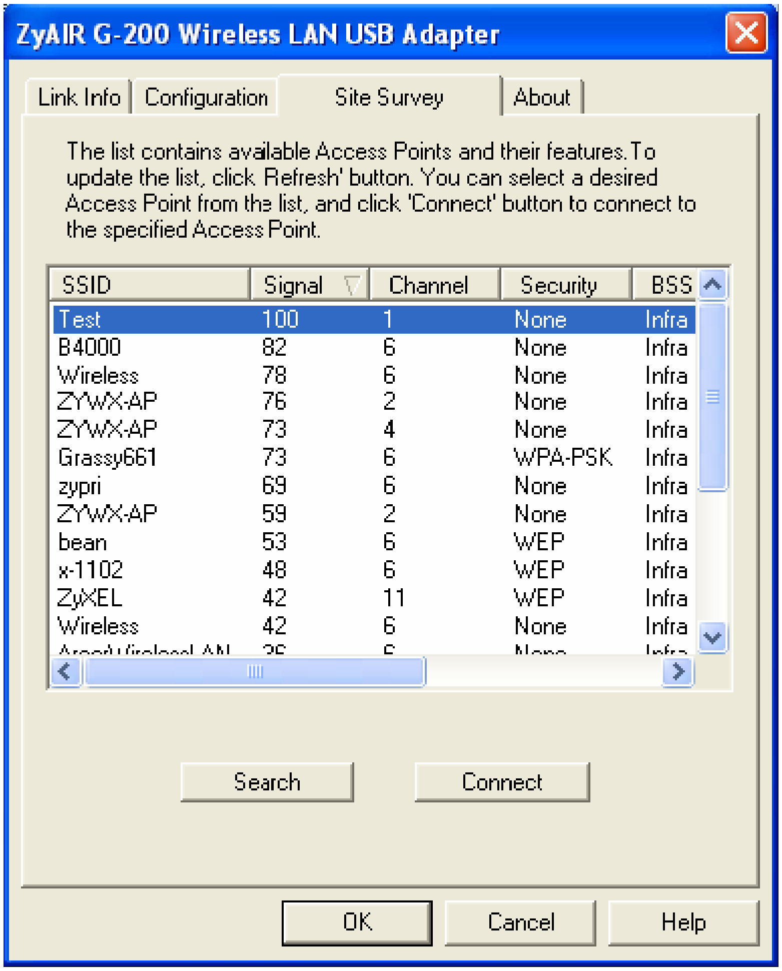
Service Set Identifier: any

Operating Mode: Infrastructure

Channel: 8

Step 3: Select Infrastructure from the operation mode pull down menu. You can fill in an SSID or leave it set as “any”, if you wish to connect to any AP. Press Apply Changes for settings to take effect.

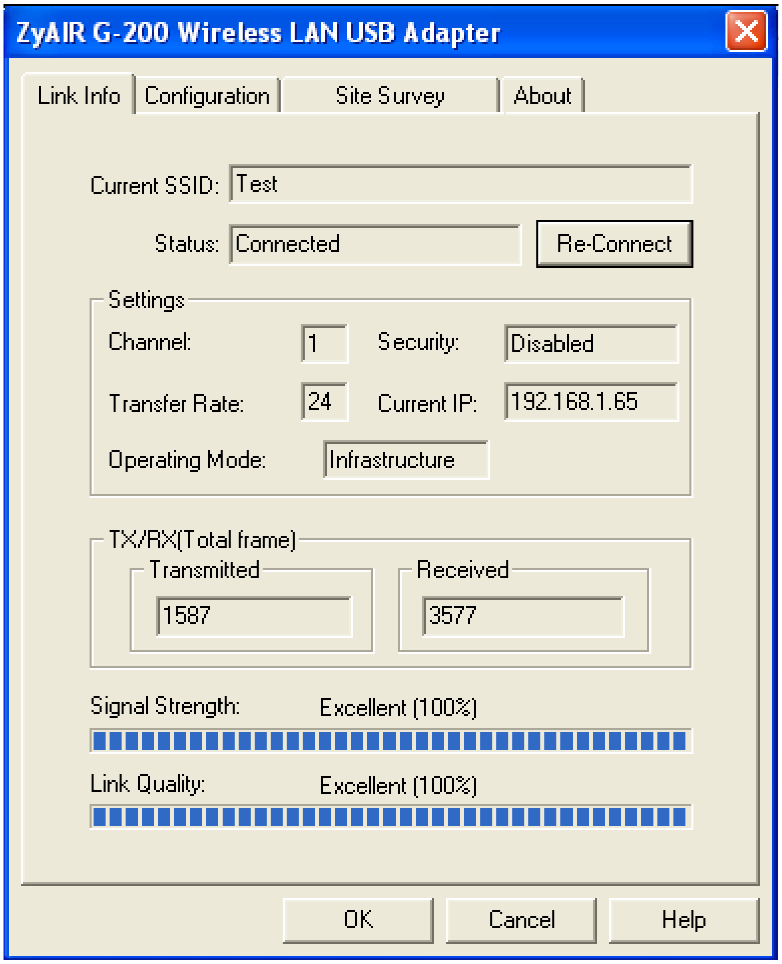
Step 4: Click on the Site Survey tab, and press search. All the available APs will be listed.



The list contains available Access Points and their features. To update the list, click Refresh' button. You can select a desired Access Point from the list, and click 'Connect' button to connect to the specified Access Point.

SSID	Signal	Channel	Security	BSS
Test	100	1	None	Infra
B4000	82	6	None	Infra
Wireless	78	6	None	Infra
ZYWX-AP	76	2	None	Infra
ZYWX-AP	73	4	None	Infra
Grassy661	73	6	WPA-PSK	Infra
zypri	69	6	None	Infra
ZYWX-AP	59	2	None	Infra
bean	53	6	WEP	Infra
x-1102	48	6	WEP	Infra
ZyXEL	42	11	WEP	Infra
Wireless	42	6	None	Infra
AreaWirelessLAN	35	6	None	Infra

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



Current SSID: Test

Status: Connected

Settings

Channel: 1

Security: Disabled

Transfer Rate: 24

Current IP: 192.168.1.65

Operating Mode: Infrastructure

TX/RX(Total frame)

Transmitted: 1587

Received: 3577

Signal Strength: Excellent (100%)

Link Quality: Excellent (100%)

Step 6: After the client have associated with the selected AP successfully in the infrastructure mode, the linked AP's channel, current linkup rate, SSID, link quality, and signal strength will show on the Link Info page.

2. MAC Filter

MAC Filter Overview

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

• ZyXEL MAC Filter Implementation

ZyXEL's MAC Filter Implementation allows users to define a list of the MAC addresses that are allowed for or blocked from association with STAs. The filter settings allow users to input 12 entries in the list. If Allow Association is selected, all the 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.

- **Configuring 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 you don't know what your MAC address is, enter a command "ipconfig /all" in the 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 with 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 the wireless LANs.

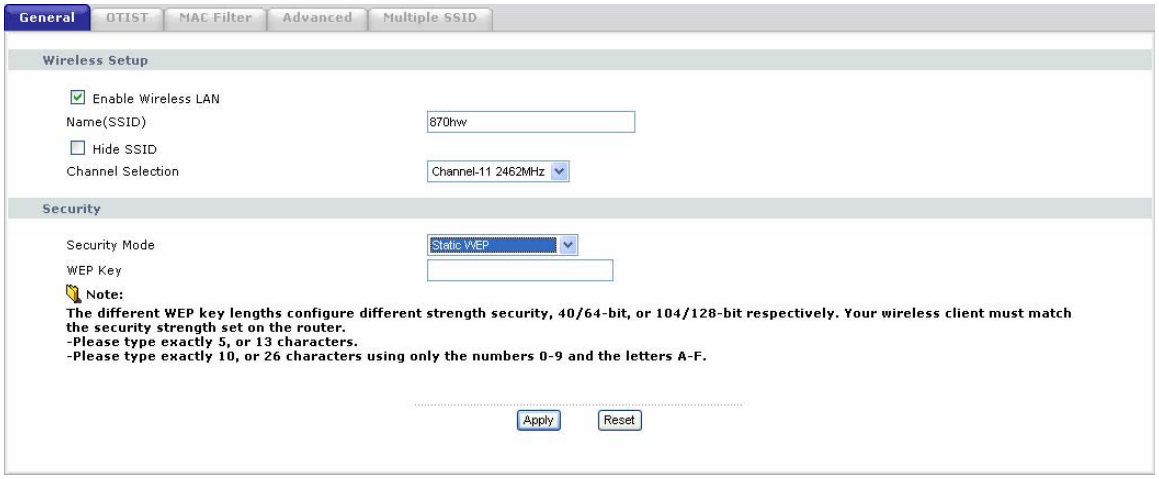
The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. WEP is implemented because wireless transmissions are easier to intercept than transmissions over wired networks, as wireless transmission is a shared medium, everything that is transmitted or received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

- **Setting up the Access Point**

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

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



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): 870hw

□ Hide SSID

Channel Selection: Channel-11 2462MHz

Security

Security Mode: Static WEP

WEP Key:

Note:
The different WEP key lengths configure different strength security, 40/64-bit, or 104/128-bit respectively. Your wireless client must match the security strength set on the router.
-Please type exactly 5, or 13 characters.
-Please type exactly 10, or 26 characters using only the numbers 0-9 and the letters A-F.

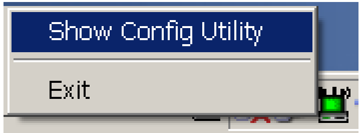
Step 2: Set up WEP Key in the Web Configurator. You need to set one of the following parameters:

- 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

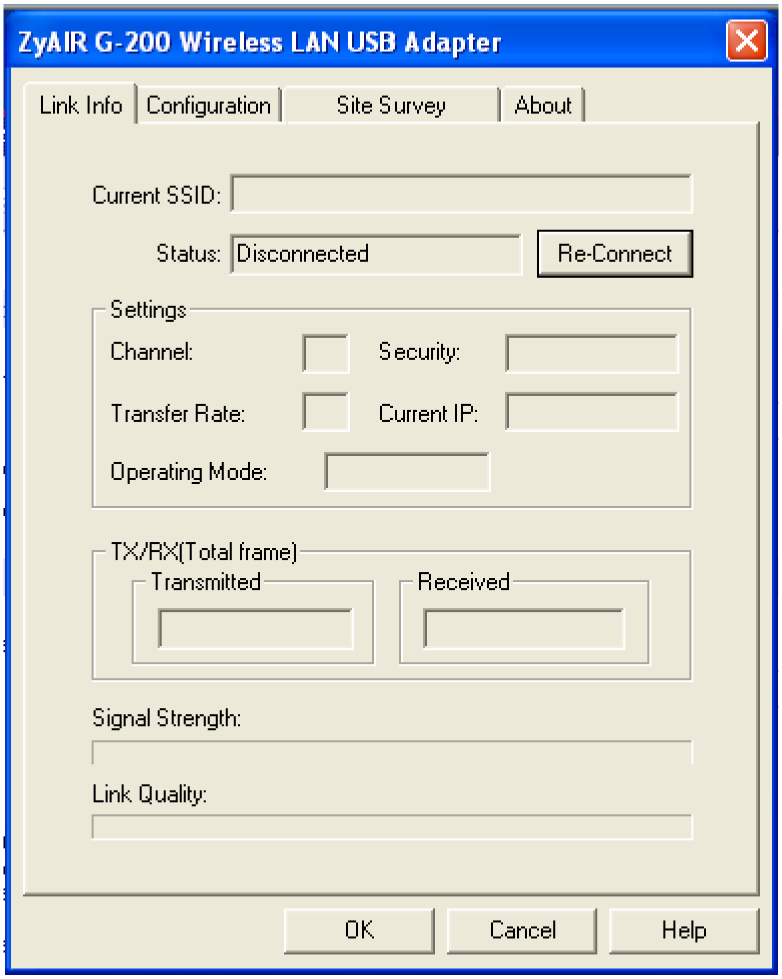
You can enter a special WEP key in the 'WEP Key' menu directly.

- **Setting up the Station**

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



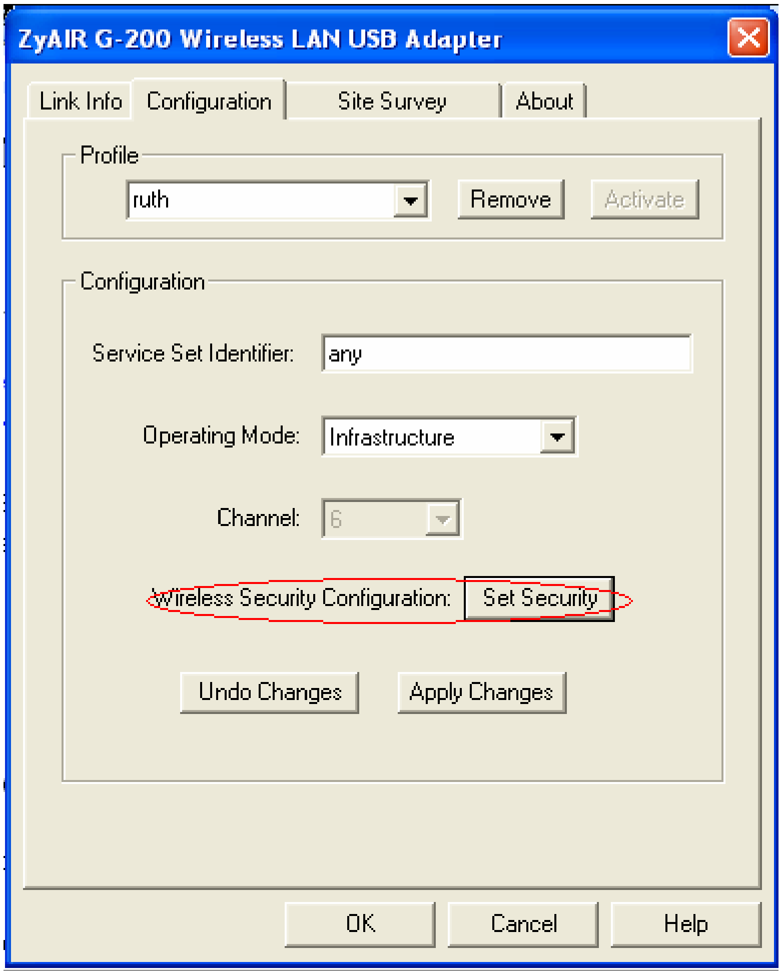
The utility screen will pop up:



Status: Disconnected

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 corresponding with those of the access point.



Profile

ruth

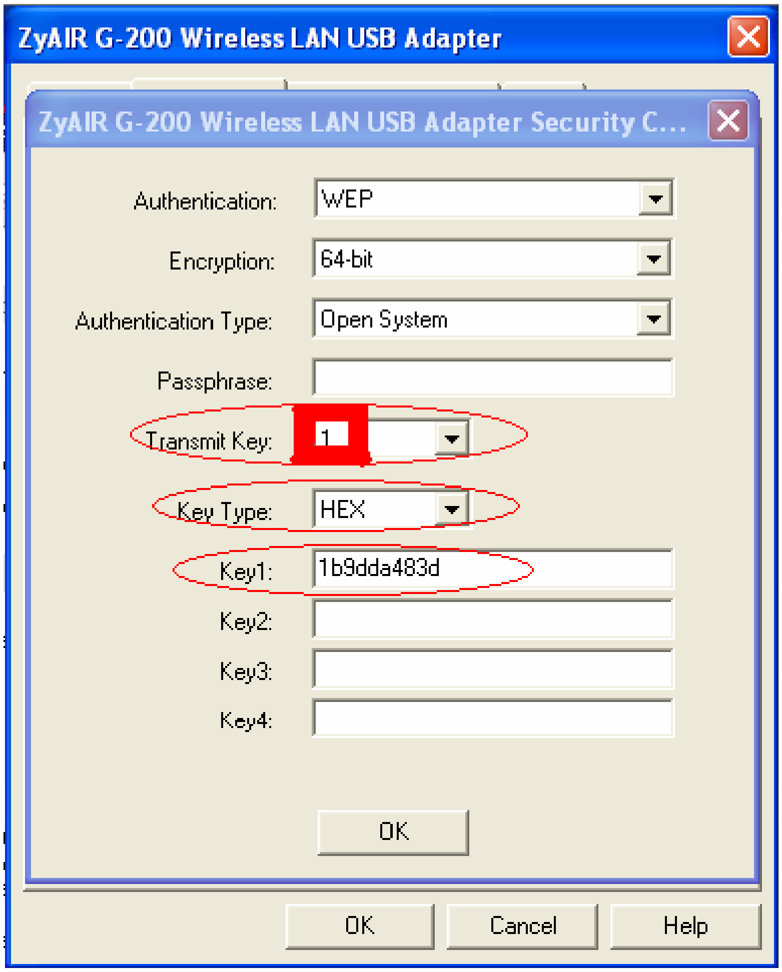
Configuration

Service Set Identifier: any

Operating Mode: Infrastructure

Channel: 6

Wireless Security Configuration: Set Security


ZyAIR G-200 Wireless LAN USB Adapter
ZyAIR G-200 Wireless LAN USB Adapter Security C...
OK
OK
Cancel
Help

Authentication: WEP

Encryption: 64-bit

Authentication Type: Open System

Passphrase:

Transmit Key: 1

Key Type: HEX

Key1: 1b9dda483d

Key2:

Key3:

Key4:

Note: You should select Key 1 as default Transmit Key, since the P-870HW-I is supposed to use Key 1 by default.

As for the key settings, The WEP Encryption type of station has to be equal to the one of the access point. Select 'ASCII' Key Type for a WEP key consisting of characters or 'HEX' for a WEP key consisting of Hexadecimal digits.

Hexadecimal digits don't need to be 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 of RF contour of RF coverage in a particular facility. For 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 bring different degree of attenuation. This will cause the RF coverage pattern to be irregular and hard to predict.

Site survey can help you to overcome these problems and even provide you 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 record the results of the survey on.

2. Visually inspect the facility, walk through the facility to verify the accuracy of the diagram and mark down any large obstacle you that might affect the RF signal, e.g. metal shelf, metal desk, etc, on the diagram.

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

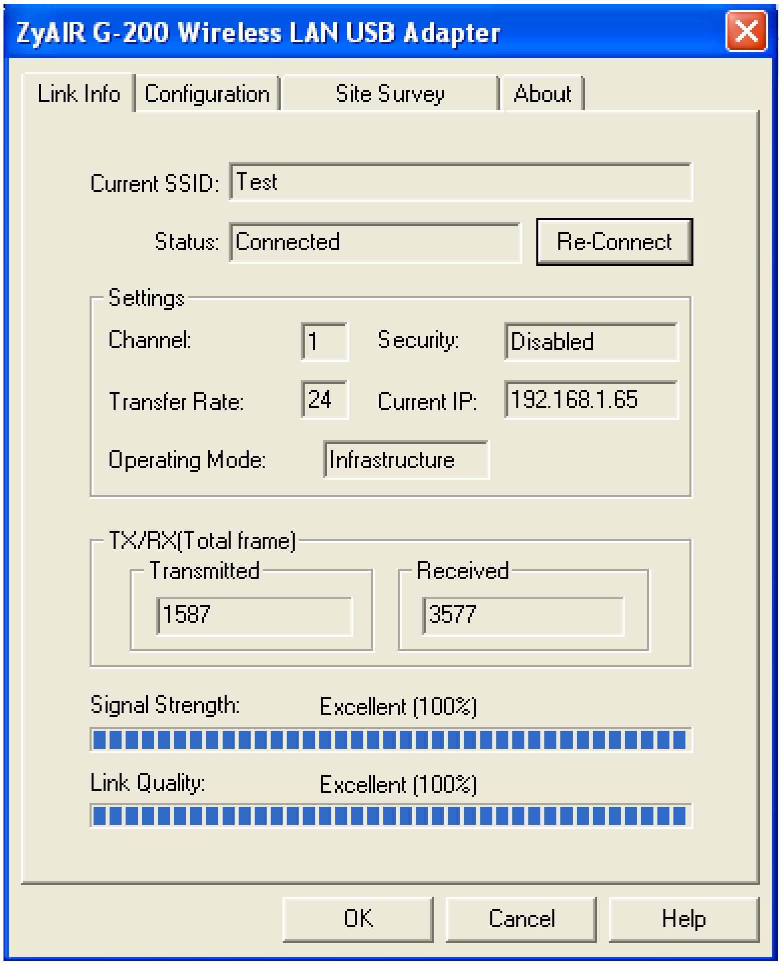
4. Determine the preliminary access point location on the facility diagram considering namely the service area needed, obstacles, power outlet location etc.

Survey on Site

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

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

Step 3: Use a notebook with wireless client installed. Open the client utility. This utility will provide information such as connection speed, currently used channel, associated rate, link quality, signal strength and other information as shown on the screen cap below.



Current SSID: Test

Status: Connected

Settings

Channel: 1

Security: Disabled

Transfer Rate: 24

Current IP: 192.168.1.65

Operating Mode: Infrastructure

TX/RX(Total frame)

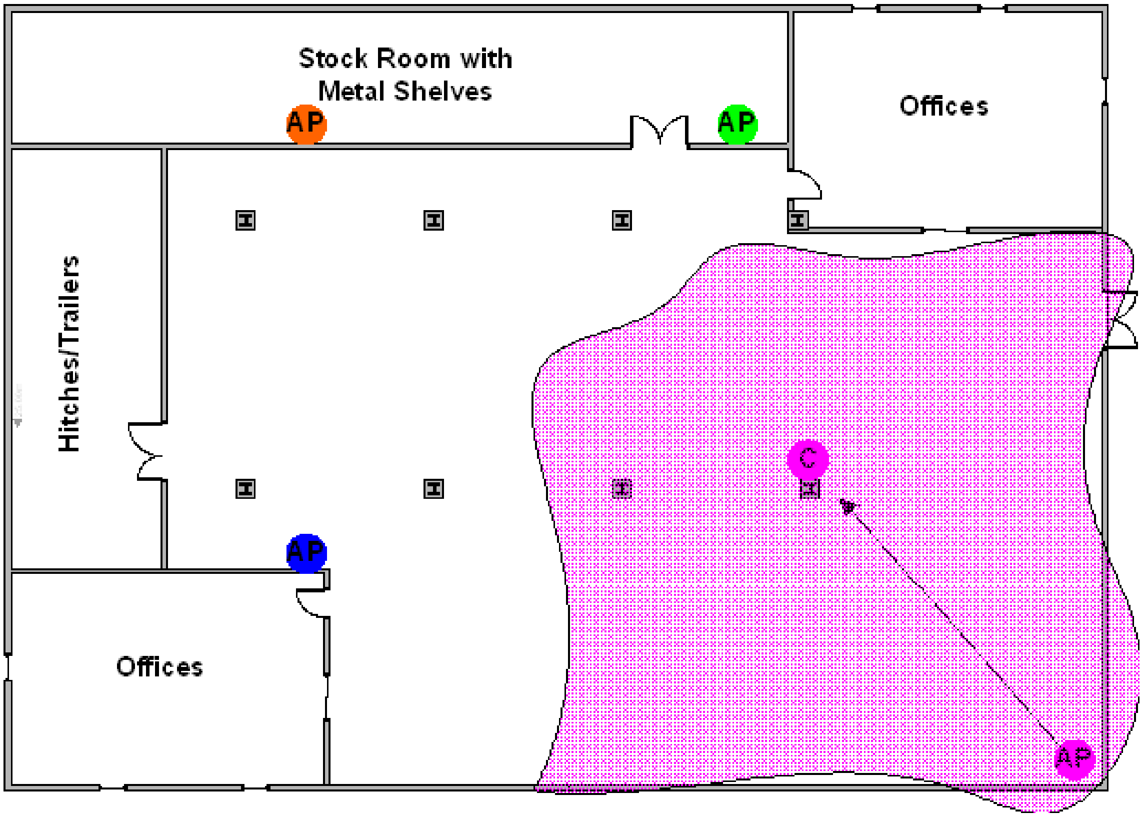
Transmitted: 1587

Received: 3577

Signal Strength: Excellent (100%)

Link Quality: Excellent (100%)

Step 4: It's always a good idea to start with putting the access point in the corner of the room and walk away from the access point in systematically. Mark down the spots where the transfer rate, the link quality and the signal strength drop below acceptable level.

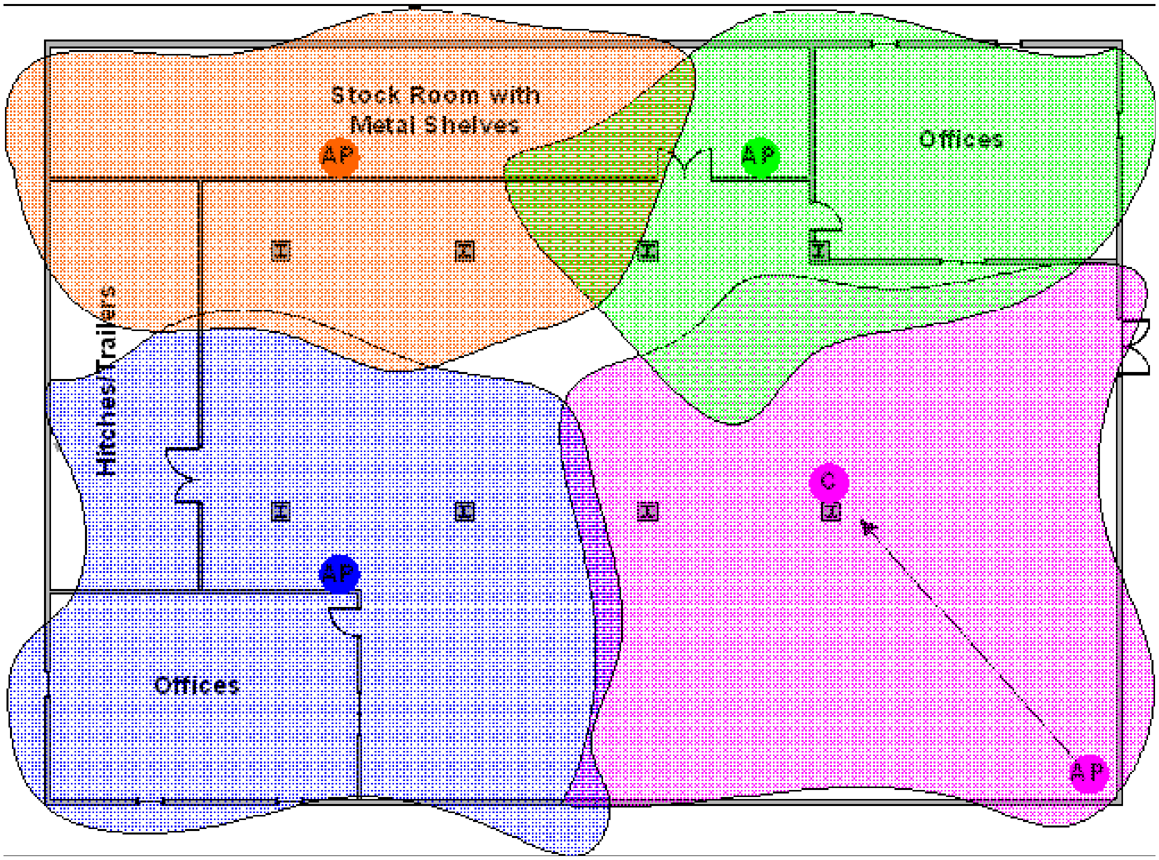


Step 5: Mark the farthest spot where the connection is still available. Now move the access point to this new spot - you have already determined the farthest access point installation spot for it to be able to provide a wireless service to the corner of the room.

Step 6: Repeat steps 1~5, Now you should be able to mark an RF coverage area as illustrated in the picture above.

Step 7: You may need more than one access point if the RF coverage area is not big enough.

Step 8: Repeat steps 1~6 of as necessary. Upon completion, you will have information represented by a diagram similar to the one in the figure below.



Note: If there are more than one access point, make sure the adjacent access point service areas overlap so the wireless station can roam.

5. Configuring 802.1x and WPA

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

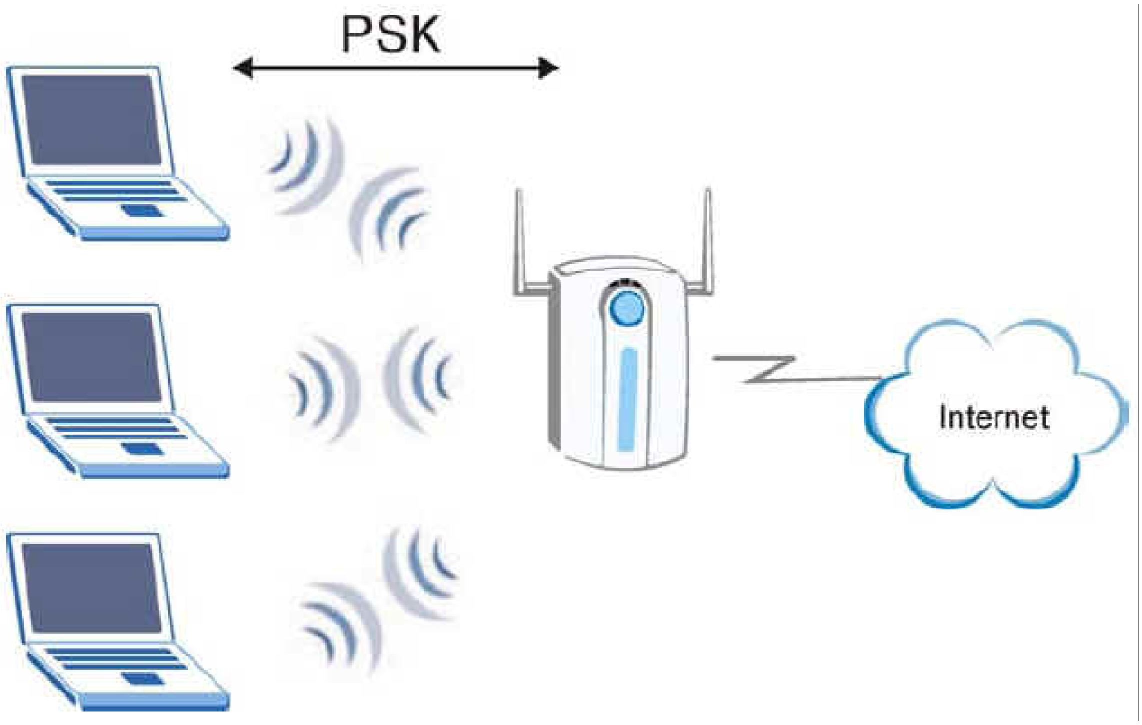
Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WAP and WEP are user authentication and improved data encryption. WAP applies IEEE 802.1x Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can not use the P-870HW-I'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 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.



- **Configuring the Access point**

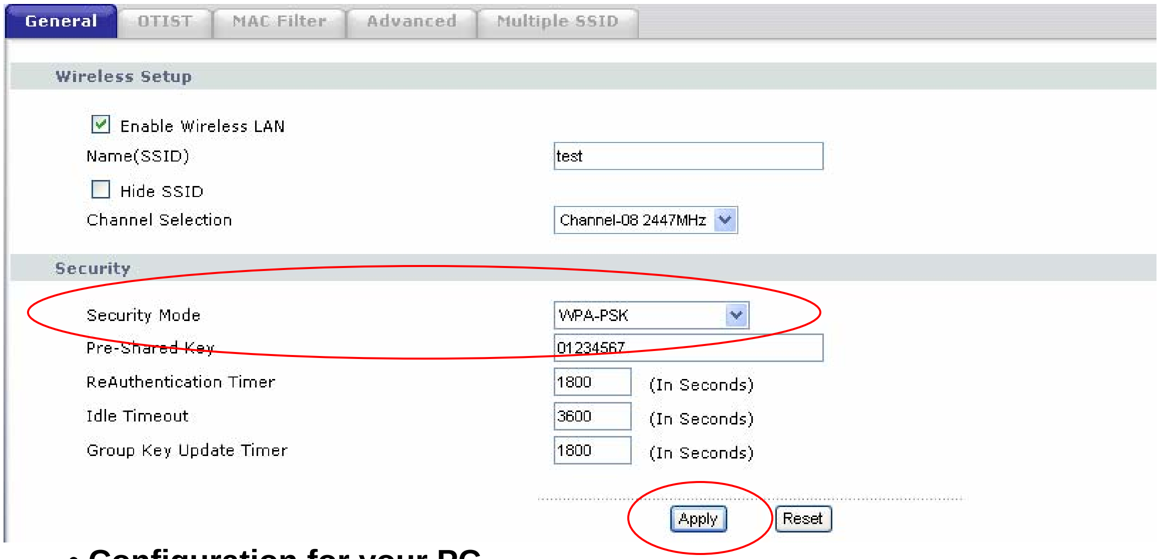
The IEEE 802.1x standard outlines enhanced security methods for both the authentication of the wireless stations and the encryption key management. Authentication can be done using local user database internal to the P-870HW-I device (authenticate up to 32 users) or using an external RADIUS server for an unlimited number of users.

Step 1: To change your P-870HW-I's authentication settings, login Web Configurator, Advanced Setup, **Network -> Wireless LAN -> General ->Security**

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.



☑ Enable Wireless LAN

Name(SSID) test

□ Hide SSID

Channel Selection Channel-08 2447MHz

Security Mode WPA-PSK

Pre-Shared Key 01234567

ReAuthentication Timer 1800 (In Seconds)

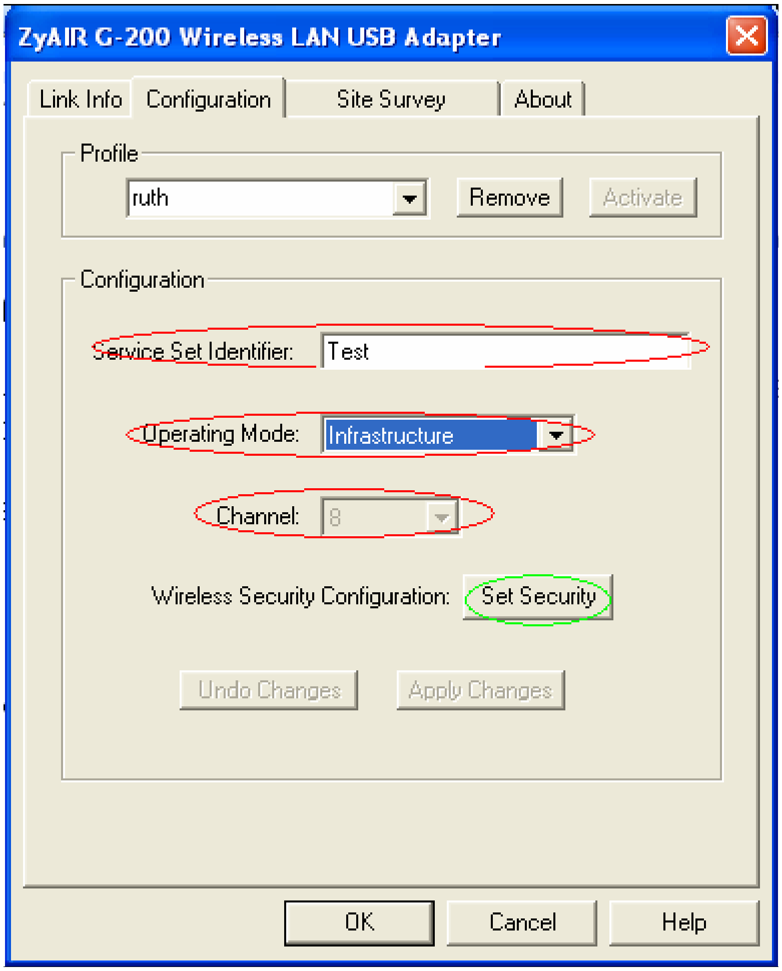
Idle Timeout 3600 (In Seconds)

Group Key Update Timer 1800 (In Seconds)

- **Configuration for your PC**

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

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



ZyAIR G-200 Wireless LAN USB Adapter

Profile: ruth

Configuration

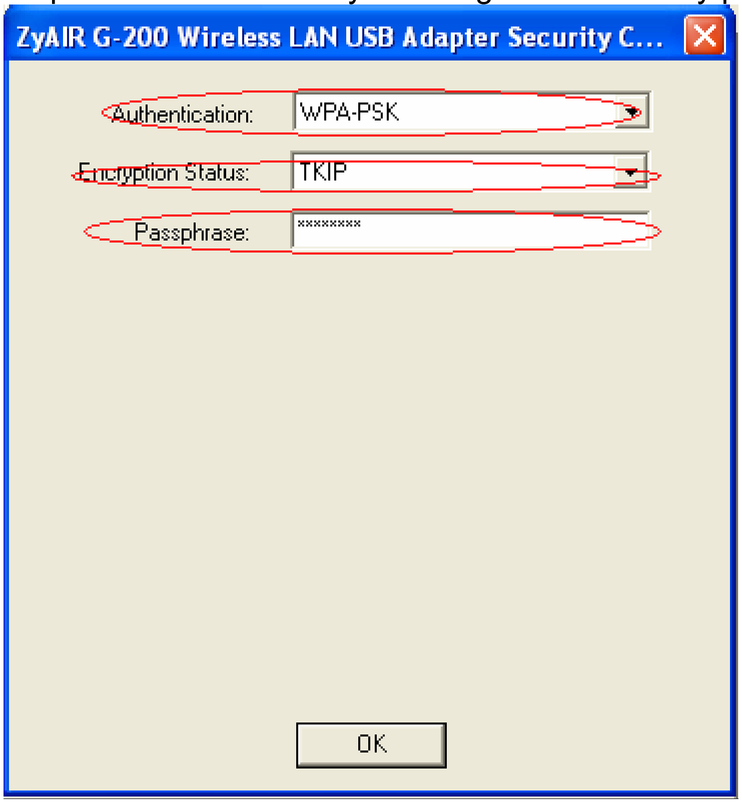
Service Set Identifier: Test

Operating Mode: Infrastructure

Channel: 8

Wireless Security Configuration: Set Security

Step 3: Click Set Security to configure the security parameters:



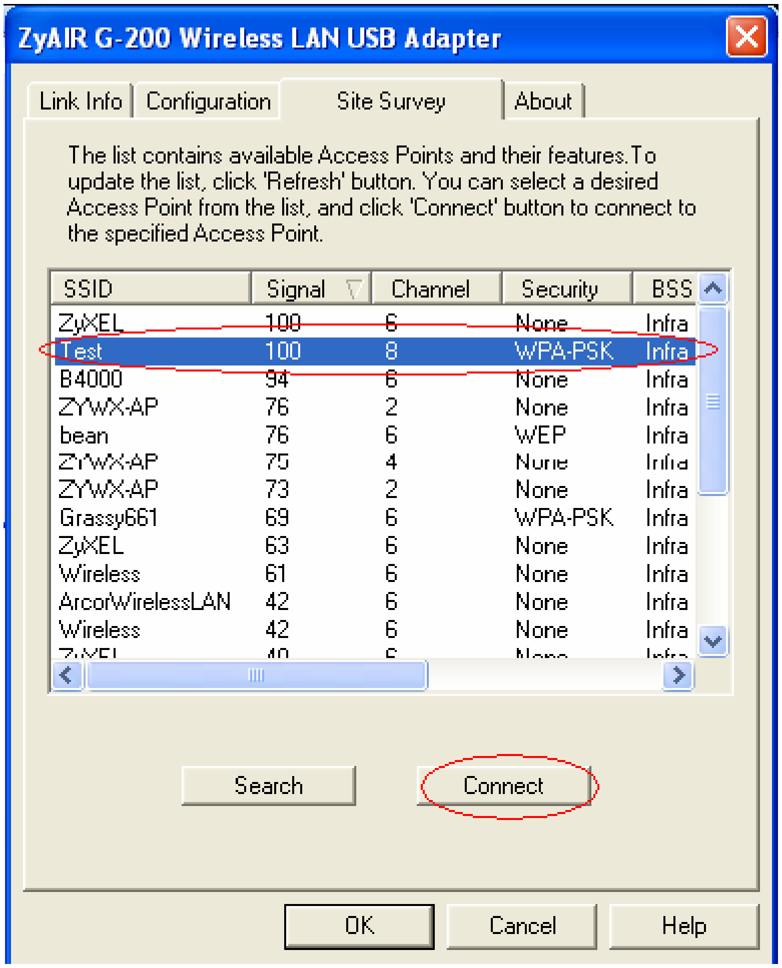
ZyAIR G-200 Wireless LAN USB Adapter Security C...

Authentication: WPA-PSK

Encryption Status: TKIP

Passphrase: *********

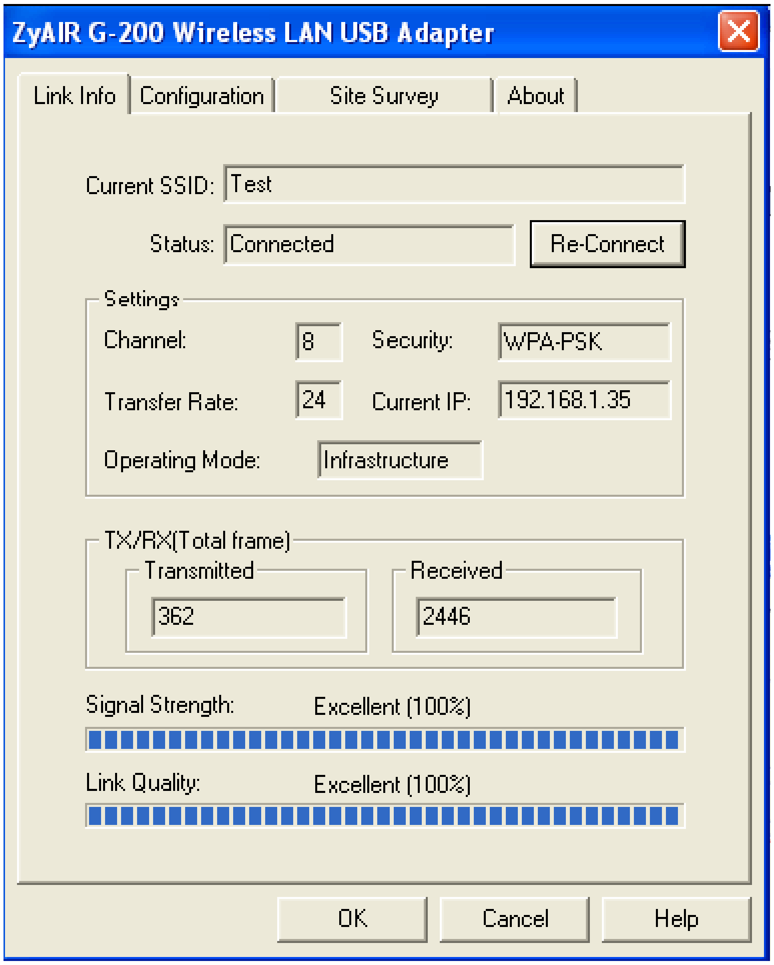
Step 4: Click OK for finish, and start the Site survey. Connect to the AP.



The list contains available Access Points and their features. To update the list, click 'Refresh' button. You can select a desired Access Point from the list, and click 'Connect' button to connect to the specified Access Point.

SSID	Signal	Channel	Security	BSS
ZyXEL	100	6	None	Infra
Test	100	8	WPA-PSK	Infra
B4000	94	6	None	Infra
ZYWX-AP	76	2	None	Infra
bean	76	6	WEP	Infra
ZYWX-AP	75	4	None	Infra
ZYWX-AP	73	2	None	Infra
Grassy661	69	6	WPA-PSK	Infra
ZyXEL	63	6	None	Infra
Wireless	61	6	None	Infra
ArcorWirelessLAN	42	6	None	Infra
Wireless	42	6	None	Infra
ZyXEL	40	6	None	Infra

Step 5: Click Link Info tab, if the PC associated and authenticated with AP successfully, you will see the following information.



Current SSID: Test

Status: Connected

Settings

Channel: 8

Security: WPA-PSK

Transfer Rate: 24

Current IP: 192.168.1.35

Operating Mode: Infrastructure

TX/RX(Total frame)

Transmitted: 362

Received: 2446

Signal Strength: Excellent (100%)

Link Quality: Excellent (100%)

6. Configure OTIST

In a wireless network, wireless clients must have the same SSID and security settings, for instance WEP (Wired Equivalent Privacy) or WPA-PSK (Wi-Fi Protected Access Pre-Share Key), as the AP (Access Point) in order to associate with it. Traditionally you have to configure the settings on the AP and then manually configure the exact same settings on each wireless client.
OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP's security settings to wireless clients that support OTIST. You can also choose to have OTIST generate a WPA-PSK key for you if you didn't configure one manually.

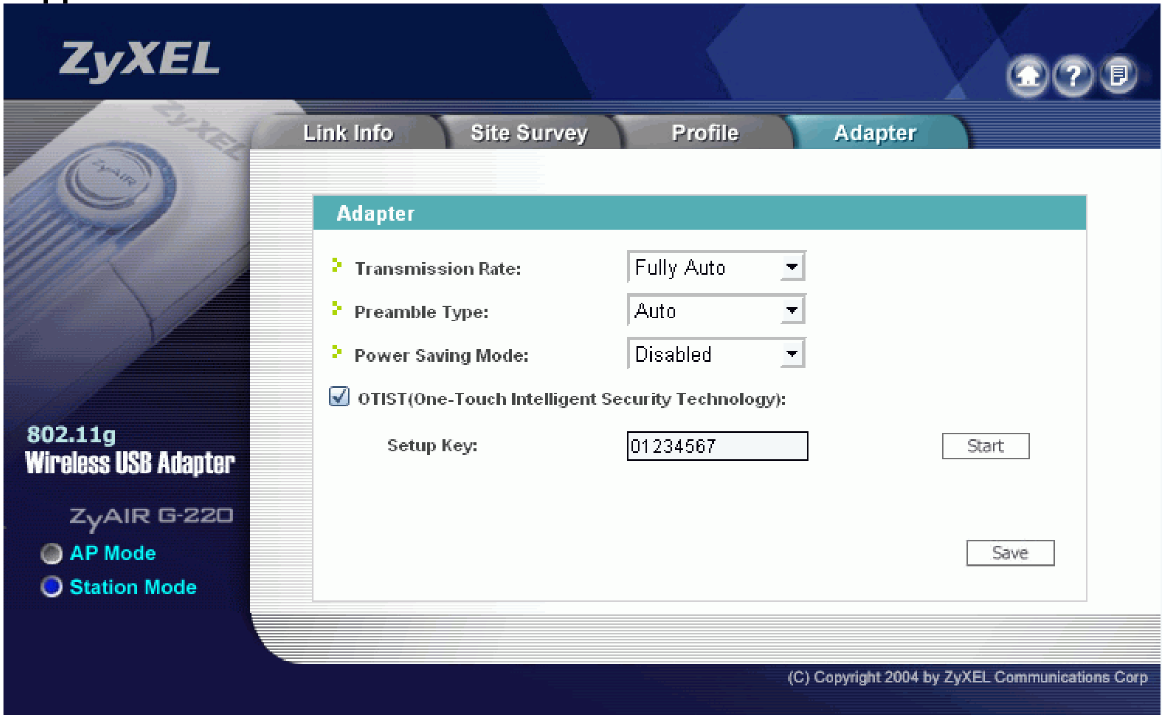
Enabling OTIST

You must activate OTIST on both the AP and wireless client before transferring configuration.
Note: The AP and wireless client MUST use the same setup key.

Wireless Client Configuration

In the wireless client ZyXEL Utility, click **Adaptor** and select the **OTIST** check box. Enter the same Setup Key as you predefined in the AP. Click on **Save** to save the configuration.

Note: At the time of writing, ZyXEL wireless clients G-162, G-360 and G-220 support OTIST.



Adapter

Transmission Rate: Fully Auto

Preamble Type: Auto

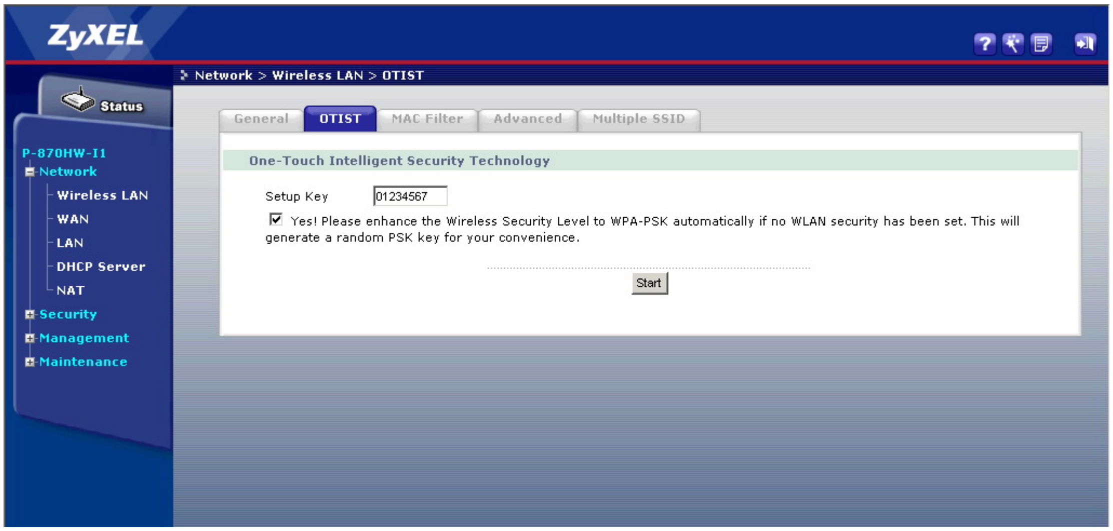
Power Saving Mode: Disabled

☑ OTIST(One-Touch Intelligent Security Technology):

Setup Key: 01234567

Access Point Configuration

You can activate OTIST by either pressing a button on the device panel or through the web configuration. In this example, the web configurator method is shown.
Step1. Open a web browser window and login into the web configurator.
Step2. Click **Network** > **Wireless LAN** > **OTIST** and specify the Setup Key (up to 8 characters, for instance 01234567). To have OTIST automatically generate a WPA-PSK key, check the checkbox to enhance the Wireless Security Level to WPA-PSK automatically, it no WLAN security has been set. Note: If you manually configure a WEP key or a WPA-PSK key, you can also select this check box. The ZyXEL Utility will still use the key you entered.
Step3. Click **Start** in the AP **OTIST** screen. Also start **OTIST** on a ZyXEL Wireless LAN Utility Adapter screen. These must be done within 180 seconds.



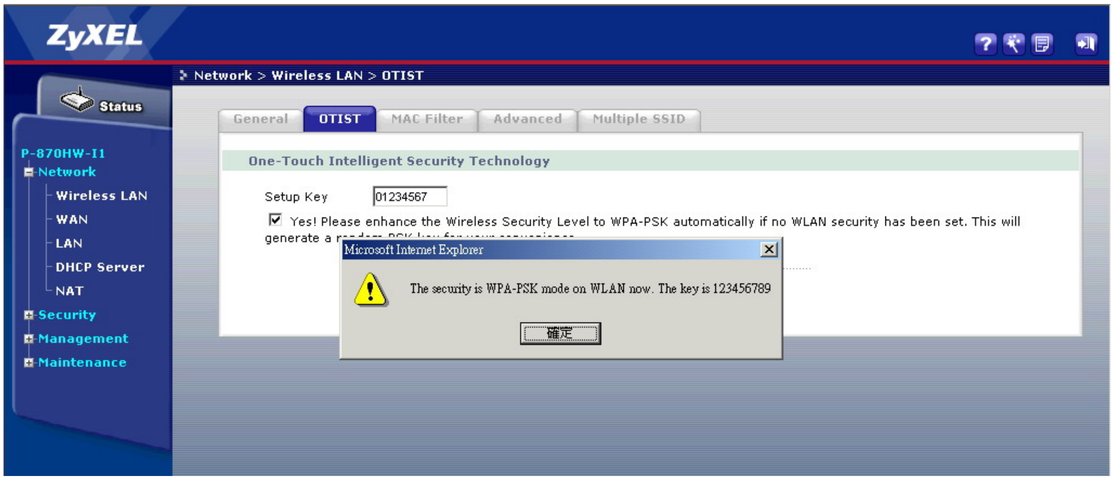
Network > Wireless LAN > OTIST

One-Touch Intelligent Security Technology

Setup Key 01234567

☑ Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience.

Step4. After pressing **Start** in the AP's **OTIST** screen, a window showing you the security settings (WPA-PSK mode and the share key is 123456789) to be transferred displays. Click **OK**.



Network > Wireless LAN > OTIST

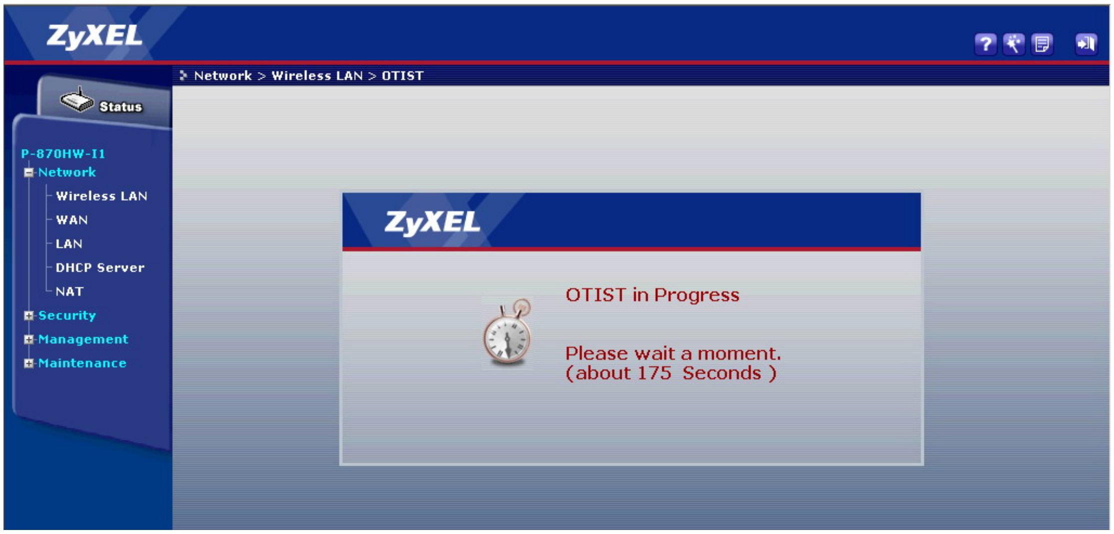
One-Touch Intelligent Security Technology

Setup Key 01234567

☑ Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a

The security is WPA-PSK mode on WLAN now. The key is 123456789

The following screen displays while the **OTIST** setting transfer is in progress. After the transfer is complete, this screen closes.



OTIST in Progress

Please wait a moment.
(about 175 Seconds)

Support Tool

1. 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 FTP client software. See the example shown below.

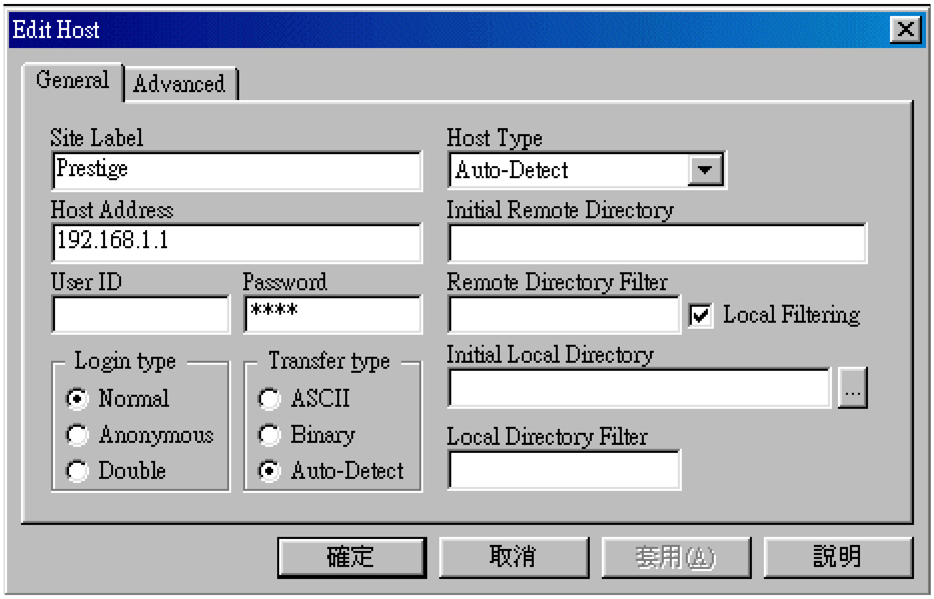
- **Using FTP client software**

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

Step 1	Use FTP client on 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'.



Site Label: Prestige

Host Type: Auto-Detect

Host Address: 192.168.1.1

Initial Remote Directory:

User ID:

Password: ****

Remote Directory Filter:

☑ Local Filtering

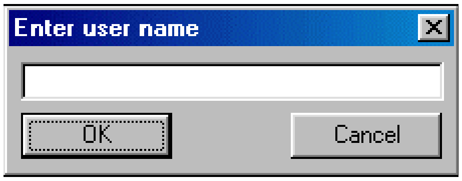
Initial Local Directory:

Login type: ● Normal ○ Anonymous ○ Double

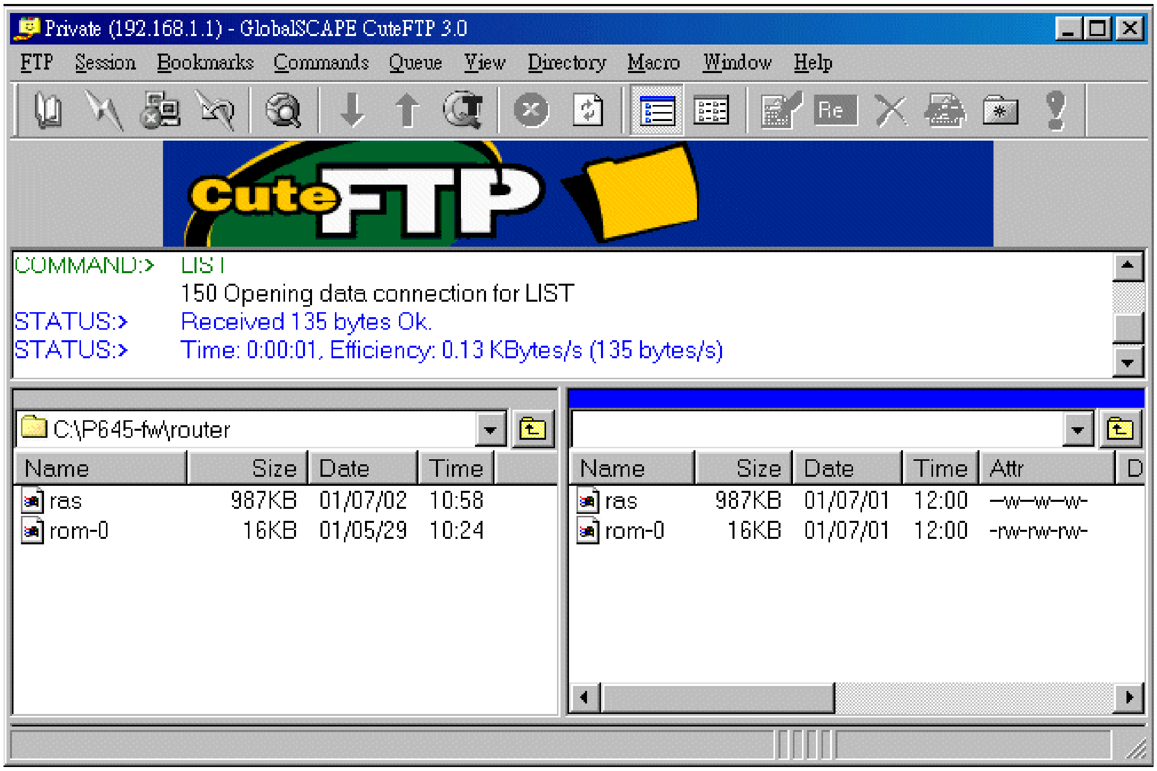
Transfer type: ○ ASCII ○ Binary ● Auto-Detect

Local Directory Filter:

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.



```
COMMAND:>  LIST
           150 Opening data connection for LIST
STATUS:>   Received 135 bytes Ok.
STATUS:>   Time: 0:00:01, Efficiency: 0.13 KBytes/s (135 bytes/s)
```

C:\P645-fw\router

Name	Size	Date	Time
ras	987KB	01/07/02	10:58
rom-0	16KB	01/05/29	10:24

Name	Size	Date	Time	Attr	D
ras	987KB	01/07/01	12:00	-w-w-w-	
rom-0	16KB	01/07/01	12:00	-rw-rw-rw-	

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