Prestige 320W

802.11g Wireless Firewall Router

Support Notes

Version v1.0

September 2005

ZyXEL

Unleash Networking Power

Application Notes

General Application Notes

Internet Connection

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

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

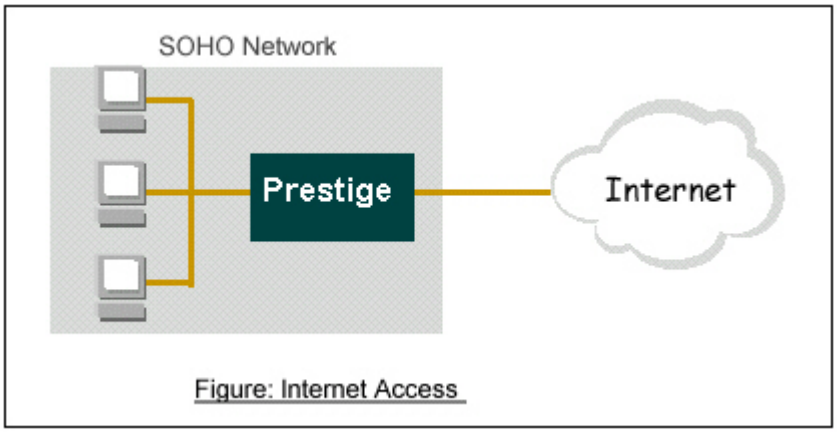


Figure: Internet Access

- Before you begin

The Prestige is shipped with the following factory default:

1. IP address = 192.168.1.1, subnet mask = 255.255.255.0 (24 bits)
2. DHCP server enabled with IP pool starting from 192.168.1.33

- Setting up the PC (Windows OS)

1. Ethernet connection

All PCs must have an Ethernet adapter card installed.

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

2. TCP/IP Installation

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

- In the **Control Panel/Network** window, click **Add** button.
- In the **Select Network Component Type** windows, select **Protocol** and click **Add**.
- In the **Select Network Protocol** windows, select **Microsoft** from the manufacturers, then select **TCP/IP** from the **Network Protocols** and click **OK**.

3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

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

Note: Do not assign arbitrary IP address and subnet mask to your PCs, otherwise, you will not be able to access the Internet.

- Click the **WINS** configuration tab and select **Disable WINS Resolution**.
- Click the **Gateway** tab. Highlight any installed gateways and click the **Remove** button until there are none listed.
- Click the **DNS Configuration** tab and select **Disable DNS**.
- Click **OK** to save and close the **TCP/IP** properties window
- Click **OK** to close the Network window. You will be prompted to insert your Windows CD or disk. When the drivers are updated, you will be asked if you want to restart the PC. Make sure your Prestige is powered on before answering Yes to the prompt. Repeat the above steps for each Windows PC on your network.

- **Setting up the Prestige router**

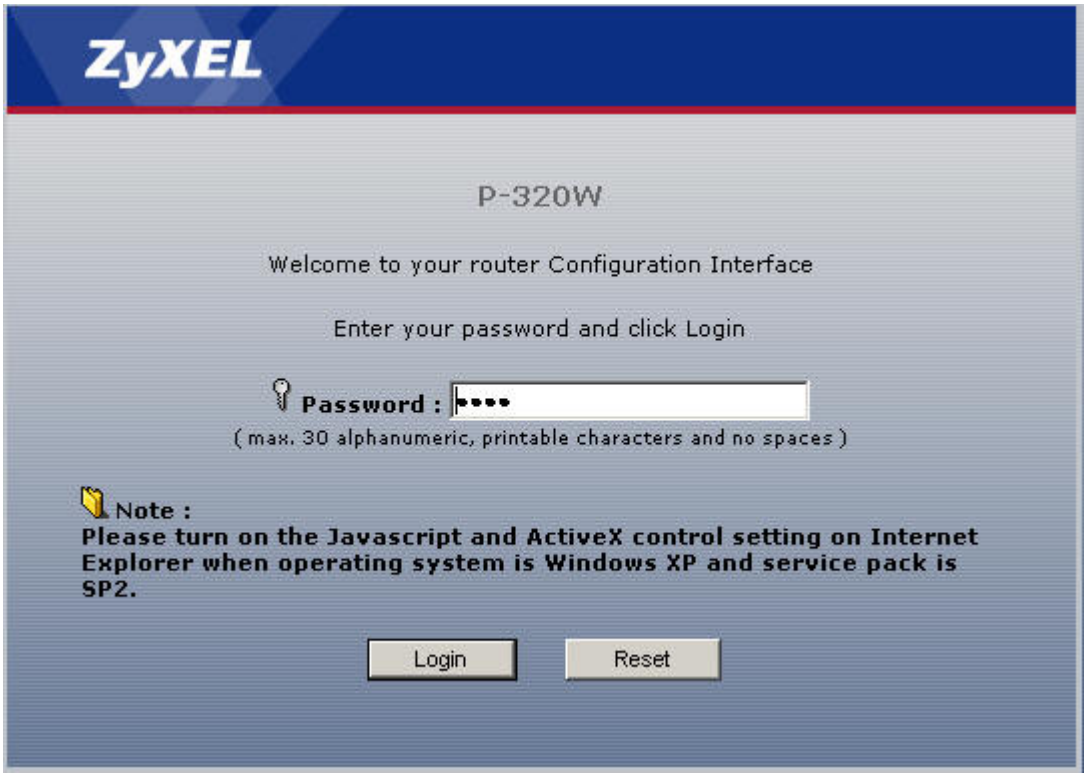
The following procedure is for the most typical usage of the Prestige where you have a single-user account (SUA). The Prestige supports embedded web server that allows you to use Web browser to configure it.

1. Retrieve Prestige Web

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

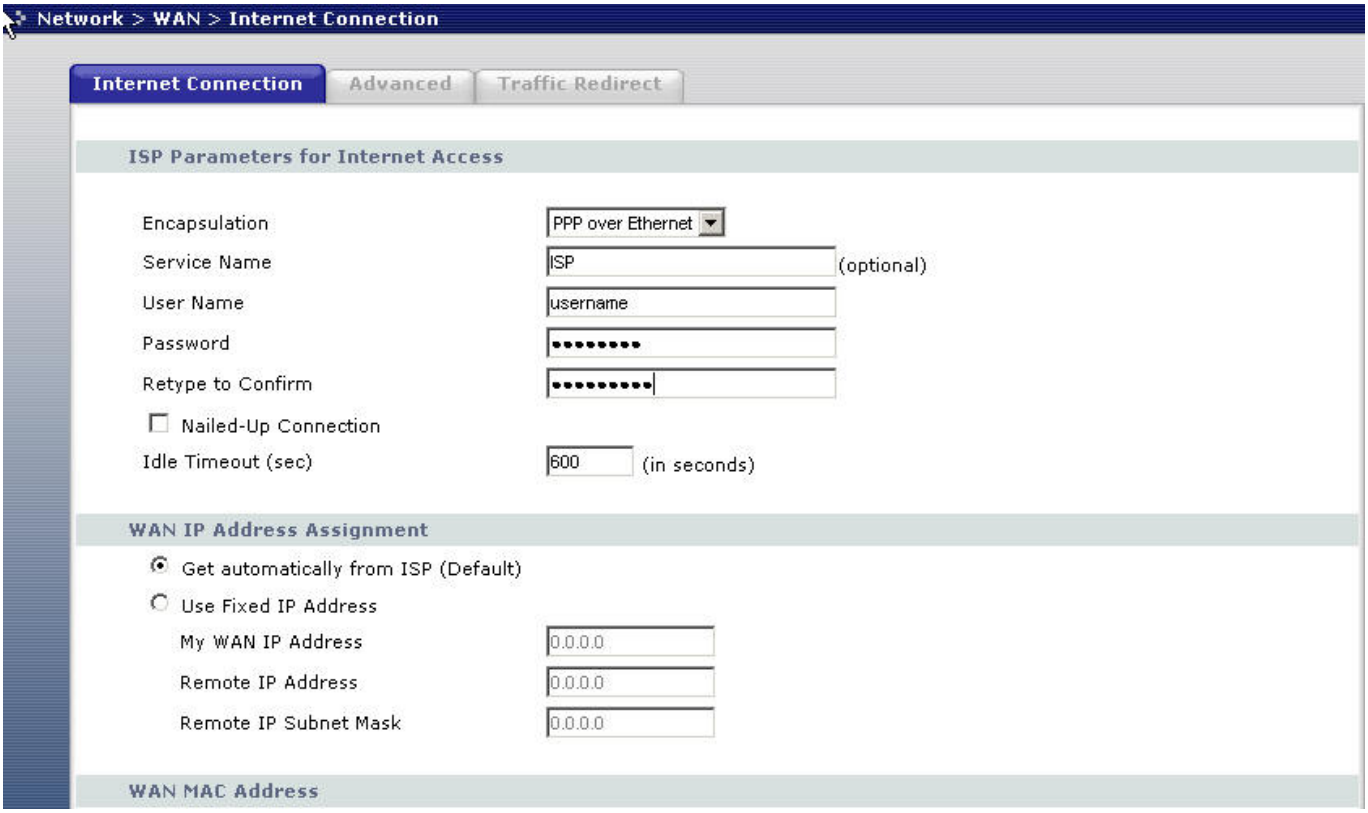
2. Login first

The default password is the '1234'.



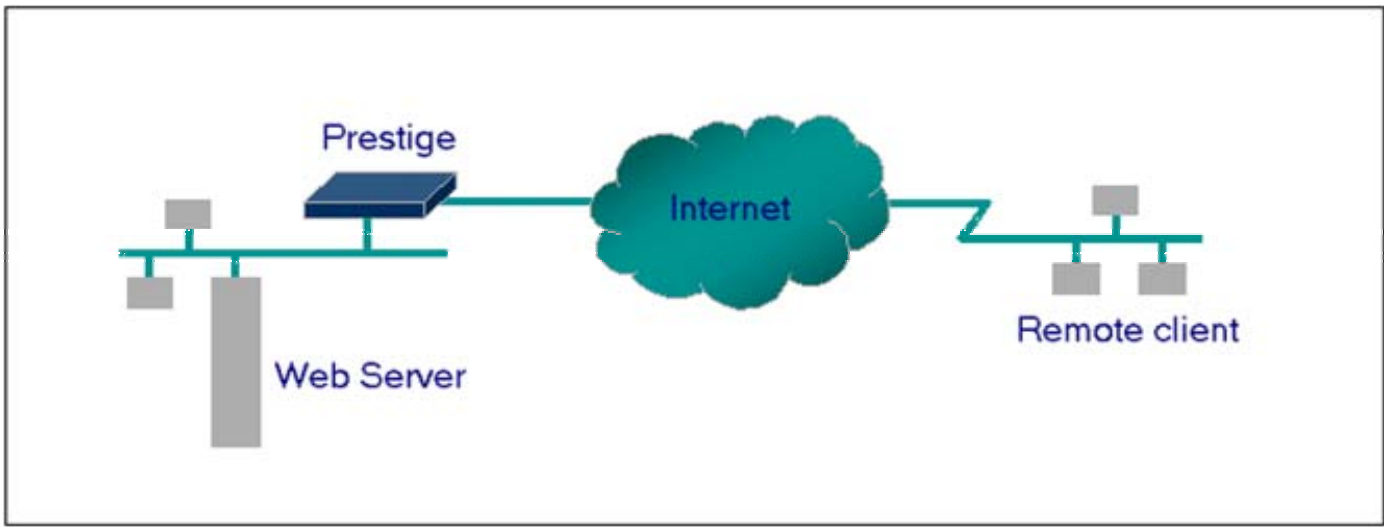
3. Configure Prestige for Internet access on Network > WAN > Internet Connection

The Web screen shown below takes PPPoE as the example.



Select "**Get automatically from ISP**" if the ISP provides the IP dynamically, otherwise select "**Use Fixed IP address**" and enter the static IP given by ISP in the box following **"MY WAN IP Address**" field.

Configure an Internal Server Behind SUA



- Introduction

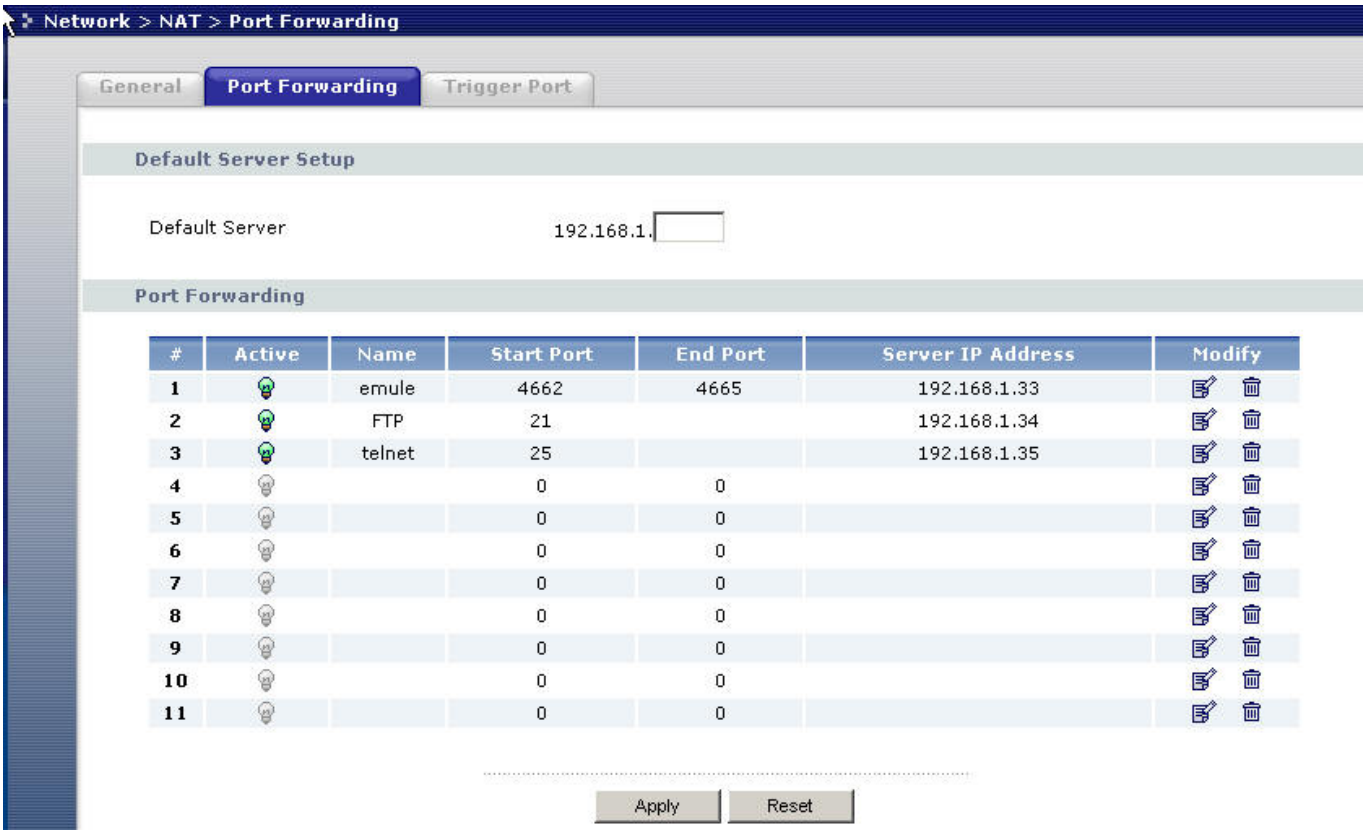
If you wish, you can make internal servers (e.g., Web, ftp or mail server) accessible for outside users, even though SUA makes your LAN appear as a single machine to the outside world. A service is identified by the port number. Also, since you need to specify the IP address of a server in the Prestige,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

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

- Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server in Network > NAT > Port Forwarding. The outside users can access the local server using the Prestige's ***WAN IP*** address.

For example (Configuring internal FTP, Telnet, and emule server for outside access) each on a different PC you would have to make configuration as follow:



- Port numbers for some common services

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

Using the Dynamic DNS (DDNS)

1. What is DDNS?

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

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

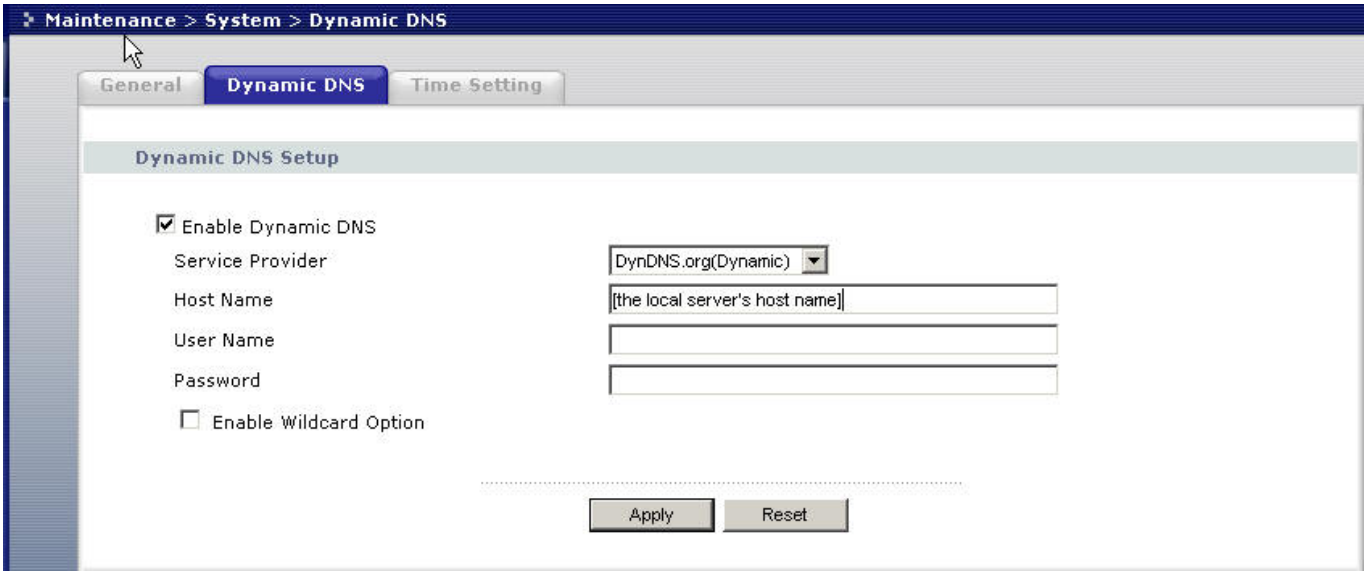
When the ISP assigns the Prestige a new IP, the Prestige must inform the DDNS server the change of this IP so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

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

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

- Setup the DDNS

- Before configuring the DDNS settings in the Prestige, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you have a hostname for your internal server and a password using to update the IP to the DDNS server.
- Go to menu Maintenance > System > Dynamic DNS to configure DDNS



Key Settings for using DDNS function:

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

Network Management Using SNMP

1. SNMP Overview

The *Simple Network Management Protocol* (SNMP) is an applications-layer protocol used to exchange the management information between network devices (e.g., routers). By using SNMP, network administrators can more easily manage network performance, find and solve network problems. The

SNMP is a member of the TCP/IP protocol suite, it uses the UDP to exchange messages between a management Client and an Agent, residing in a network node.

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

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

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

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

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

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

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

6. Reads

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

7. Writes

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

8. Traversal operations

   NMSs use these operations to determine which variables a managed device supports and to sequentially gather information from variable tables (such as IP routing table) in managed devices.

9. Traps

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

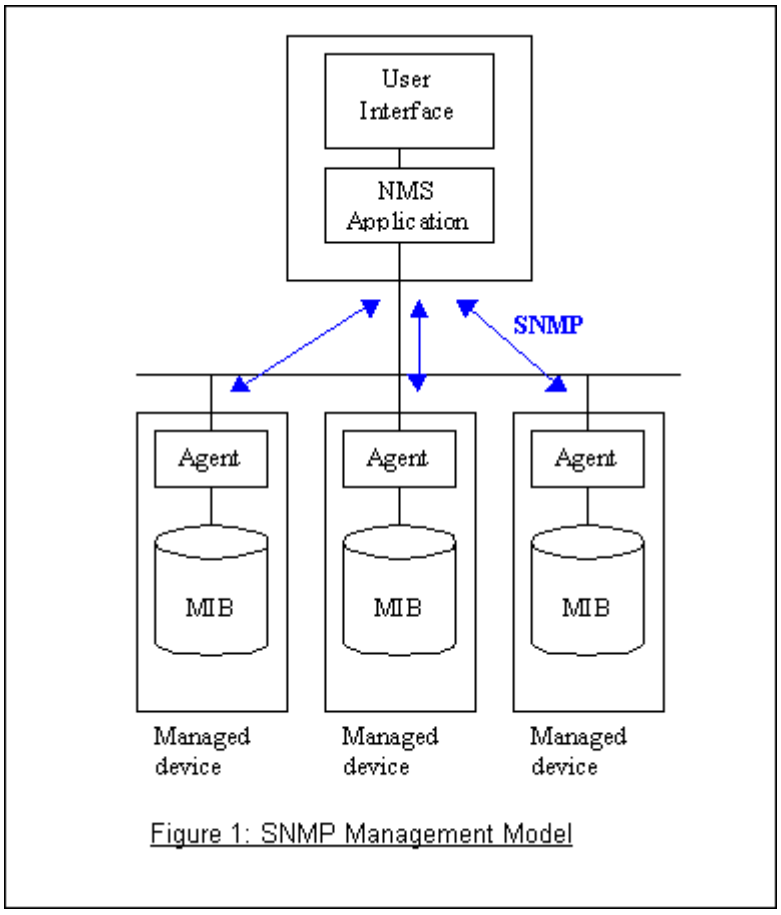


Figure 1: SNMP Management Model

2. SNMPv1 Operations

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

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

The SNMPv1 messages contains two part. The first part contains a version and a community name. The second part contains the actual SNMP protocol data unit (PDU) specifying the operation to be performed (Get, Set, and so on) and the object values involved in the operation. The following figure shows the SNMPv1 message format.

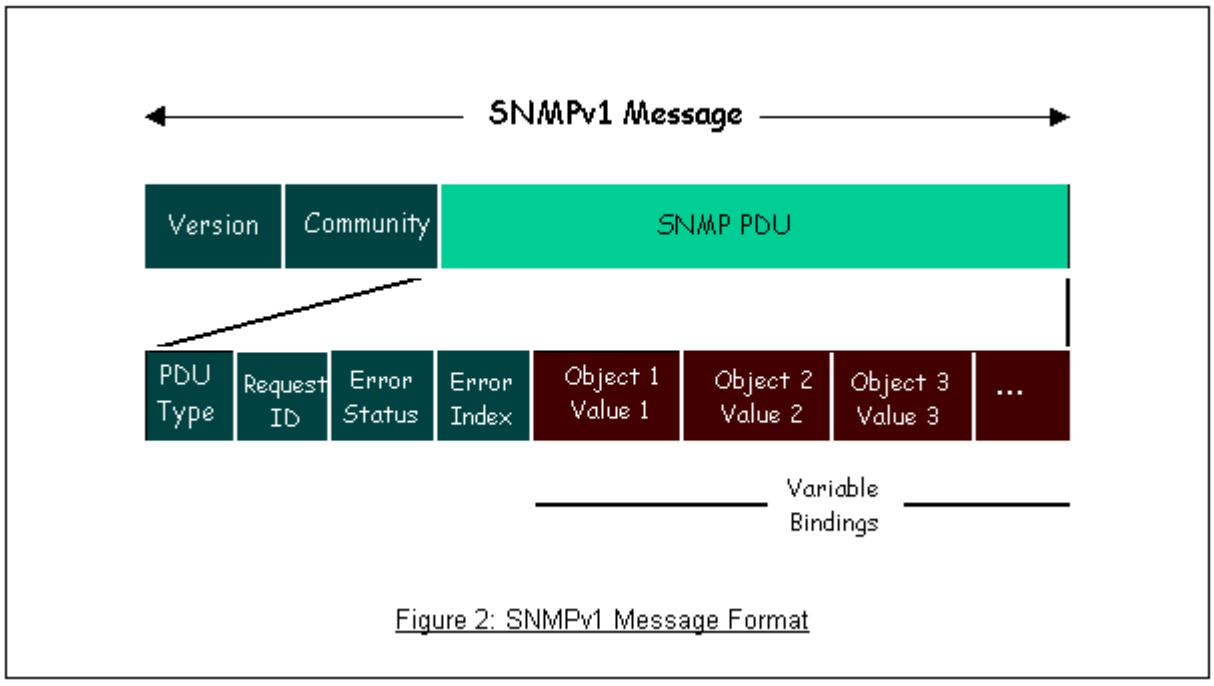


Figure 2: SNMPv1 Message Format

The SNMP PDU contains the following fields:

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

- **Variable-bindings** Associates particular object with their value.

3. ZyXEL SNMP Implementation

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

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

- coldStart (defined in RFC-1215) :

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

- warmStart (defined in RFC-1215) :

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

- linkDown (defined in RFC-1215) :

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

- linkUp (defined in RFC-1215) :

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

- authenticationFailure (defined in RFC-1215) :

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

1. whyReboot (defined in ZYXEL-MIB) :

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

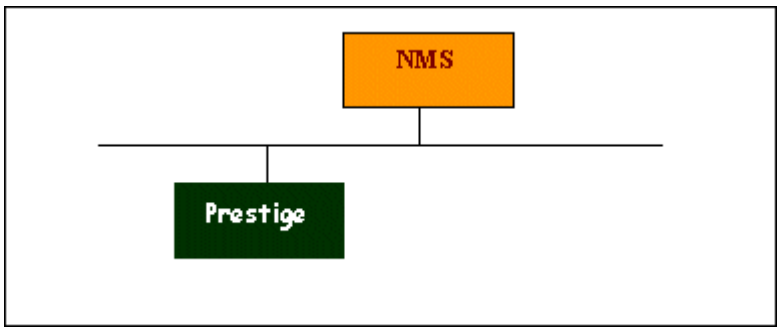
(i) For intentional reboot:

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

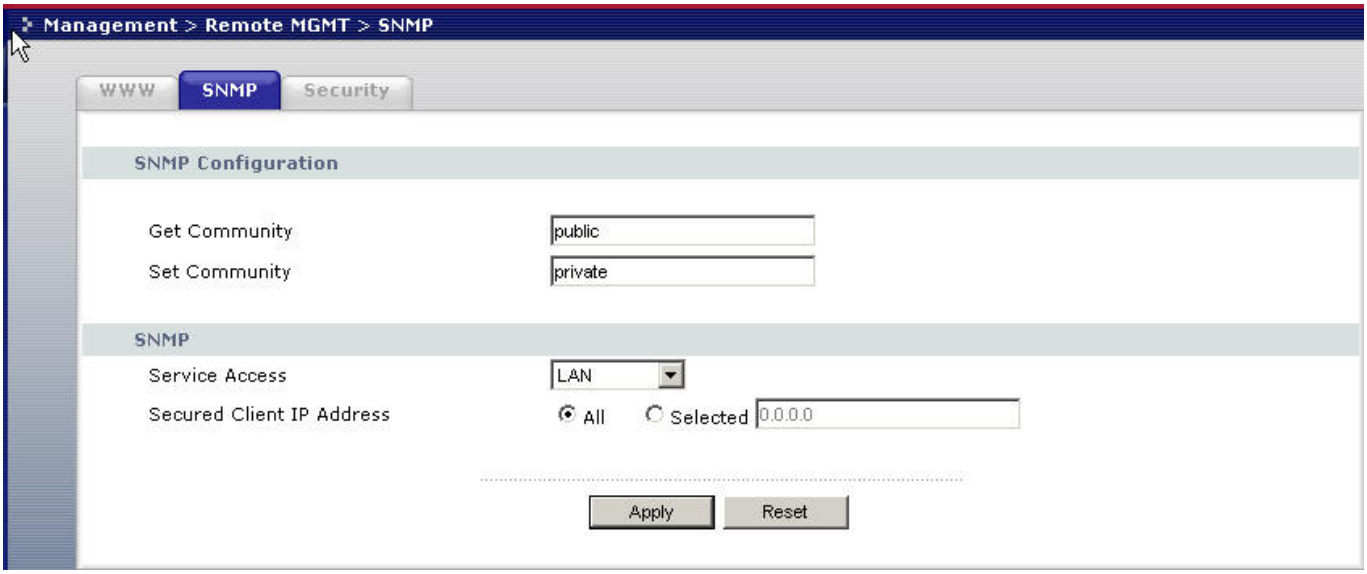
(ii) For fatal error:

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

4. Configure the Prestige for SNMP



The SNMP related settings in Prestige are configured in Management > Remote Management > SNMP The following screenshot describe a simple setup procedure for configuring all SNMP settings.



Key Settings:

Option	Descriptions
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS.

Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS.

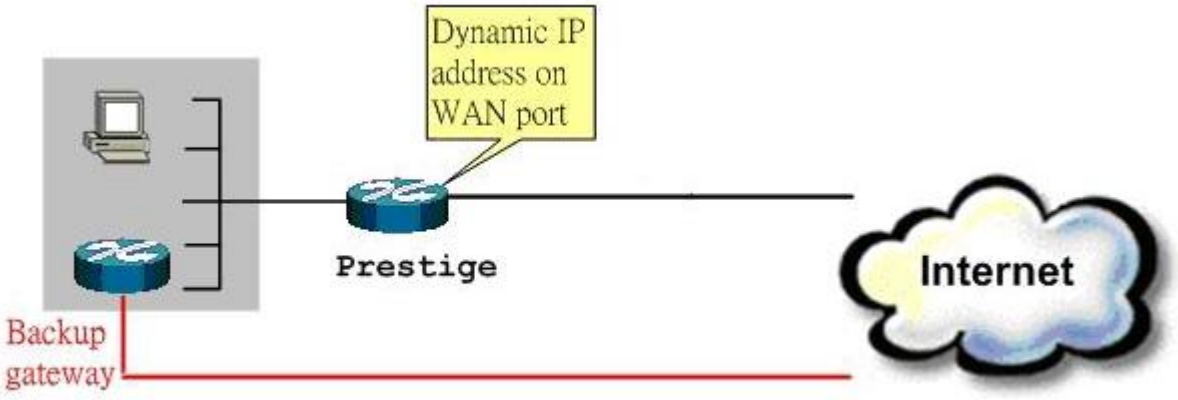
Using Prestige traffic redirect

- What is Traffic Redirect?

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

- How to deploy backup gateway?

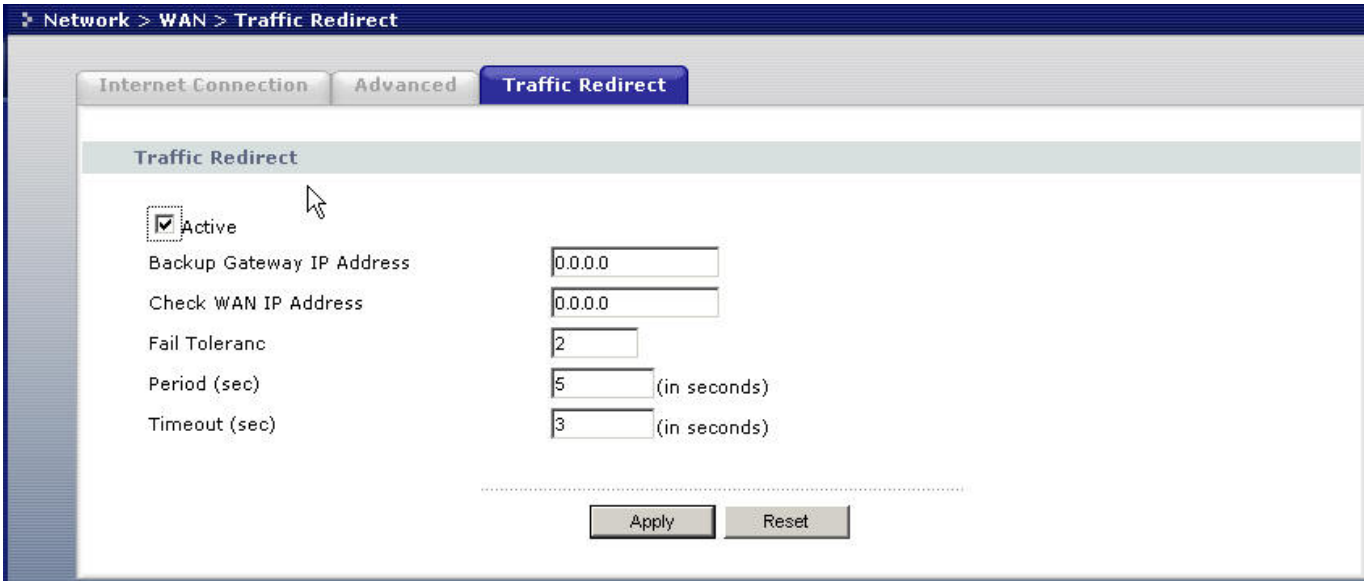
You can deploy the backup gateway on LAN of Prestige.



Traffic Redirect on LAN port

- Traffic Redirect Setup

Configure parameters that determine when Prestige will forward WAN traffic to the backup gateway using web configuration. The configuration page is in **Network > WAN > Traffic Redirect.**



Using Universal Plug n Play (UPnP)

- **1. What is UPnP**

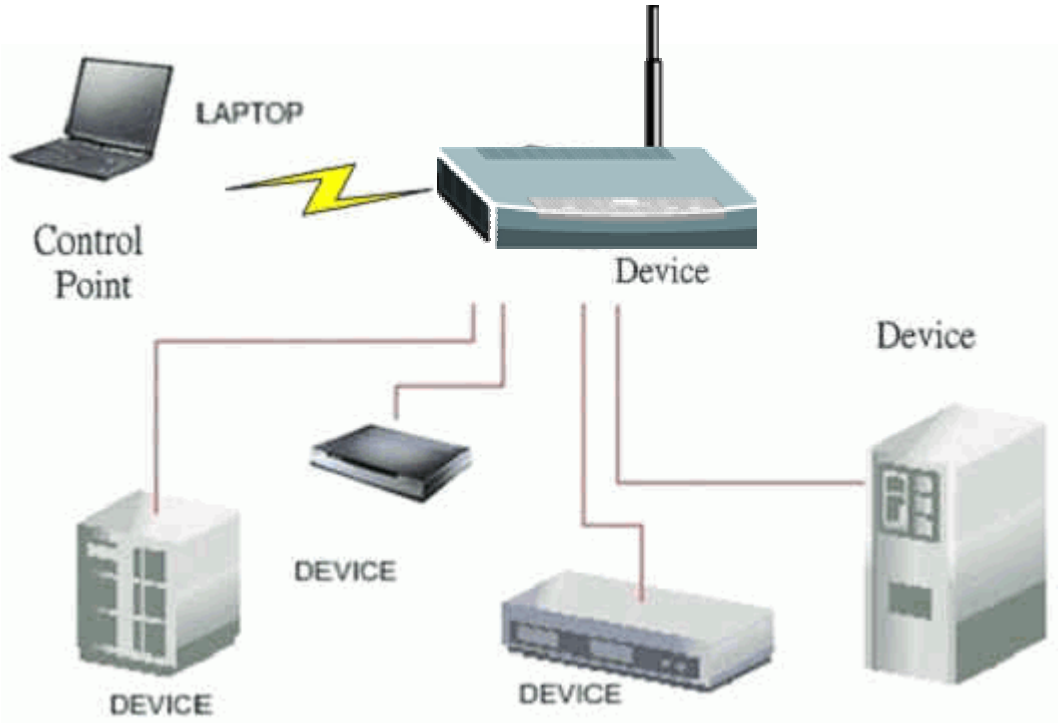
UPnP (Universal Plug and Play) makes connecting PCs of all form factors, intelligent appliances, and wireless devices in the home, office, and everywhere in between easier and even automatic by leveraging TCP/IP and Web technologies. UPnP can be supported on essentially any operating system and works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

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

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

- **Devices**: Network devices, such as networking gateways, TV, refrigerators, printers...etc, which provides services.
- **Services**: Services are provided by devices, such as time services provided by alarm clocks. In UPnP, services are described in XML format. Control points can set/get services information from devices.

- **Control points**: Control points can manipulate network devices when you add a new control point (in this case, a laptop) to a network, the device may ask the network to find UPnP-enabled devices. These devices respond with their URLs and device descriptions.



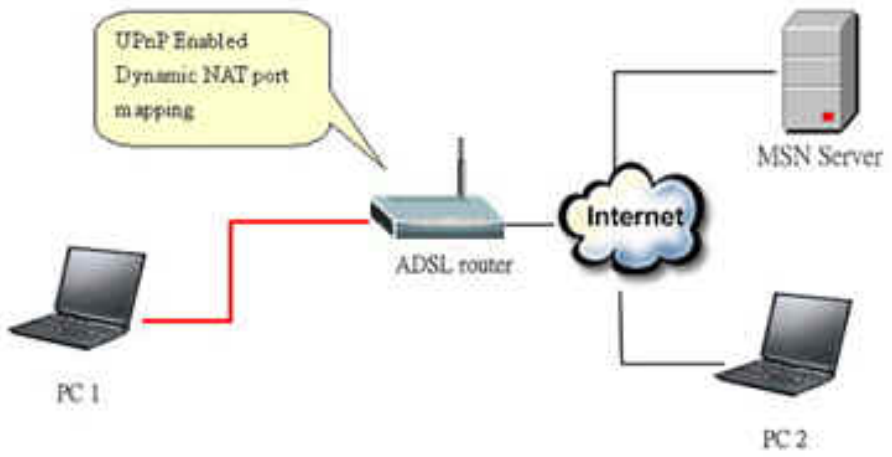
UPnP Operations

- **Addressing**: UPnPv1 devices MAY support IPv4, IPv6, or both. For IPv4, each devices should have DHCP client, when the device gets connected to the network, it will discover DHCP server on network to get an IP address. If not, then Auto-IP mechanism should be supported so that the device can give itself an IP address.(169.254.0.0/16)
- **Discovery**: Whenever a device is added on the network, it will advertise it's service over the network. Control point can also discover services provided by devices.
- **Description**: Control points can get more detailed service information from devices' description in XML format. The description may include product name, model name, serial number, vendor ID, and embedded services...etc.
- **Control**: Devices can be manipulated by control points through Control message.
- **Eventing**: Devices can send event message to notify control points if there is any update on services provided.
- **Presentation**: Each device can provide their own control interface by URL link. So that users can go to the device's presentation web page by the URL to control this device.

- **2. Using UPnP in ZyXEL devices**

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

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

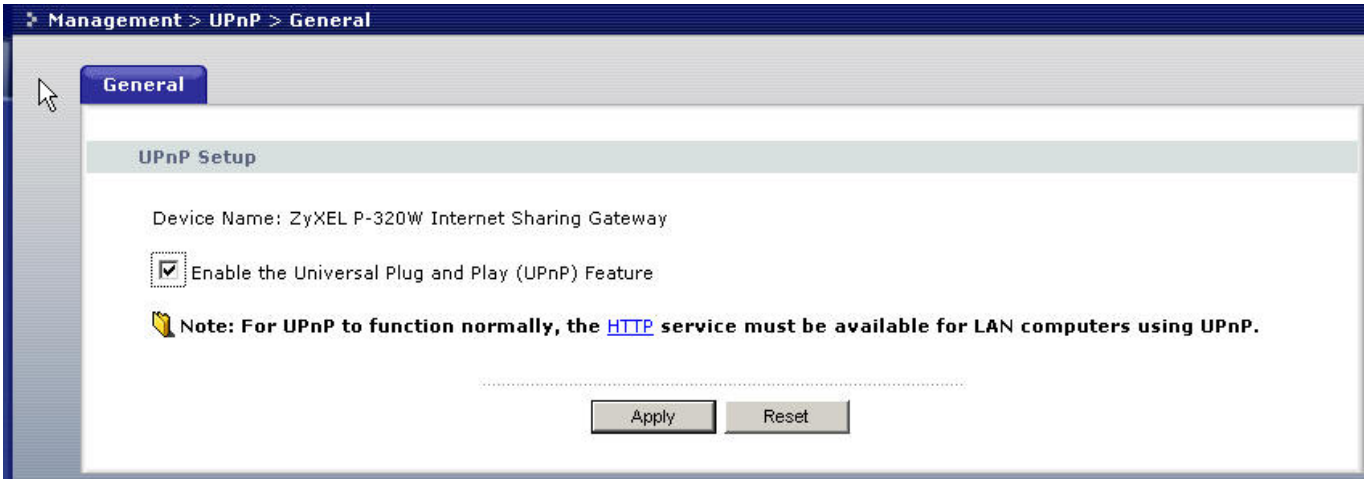


Device: P320W
Service: NAT function provided by Prestige Router
Control Point: PC1

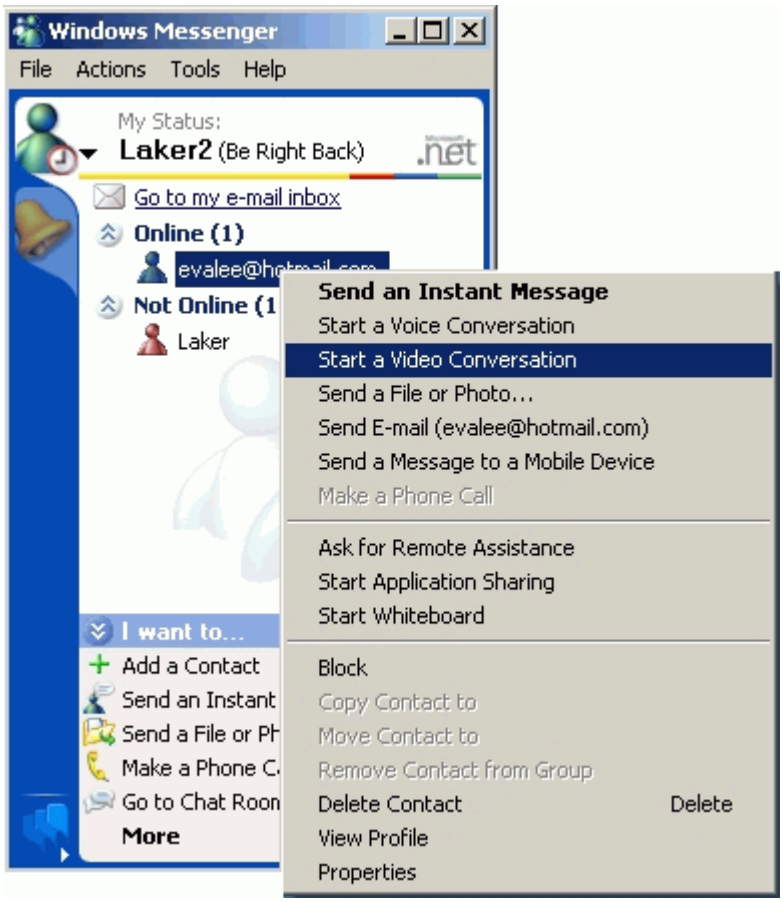
1. Enable UPnP function in ZyXEL device

Go to **Management->UPnP**, check **Enable UPnP service.**

This check box enables UPnP function in this device.

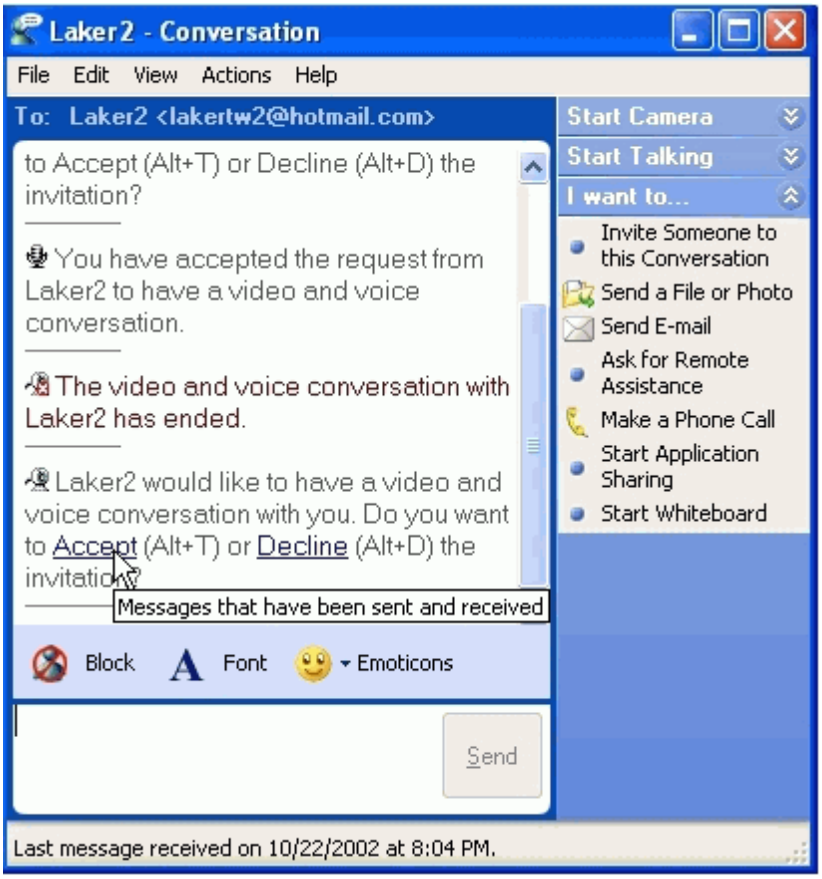


2. After getting IP address, you can go to open MSN application on PC and sign in MSN server.



3. Start a Video conversation with one online user.

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



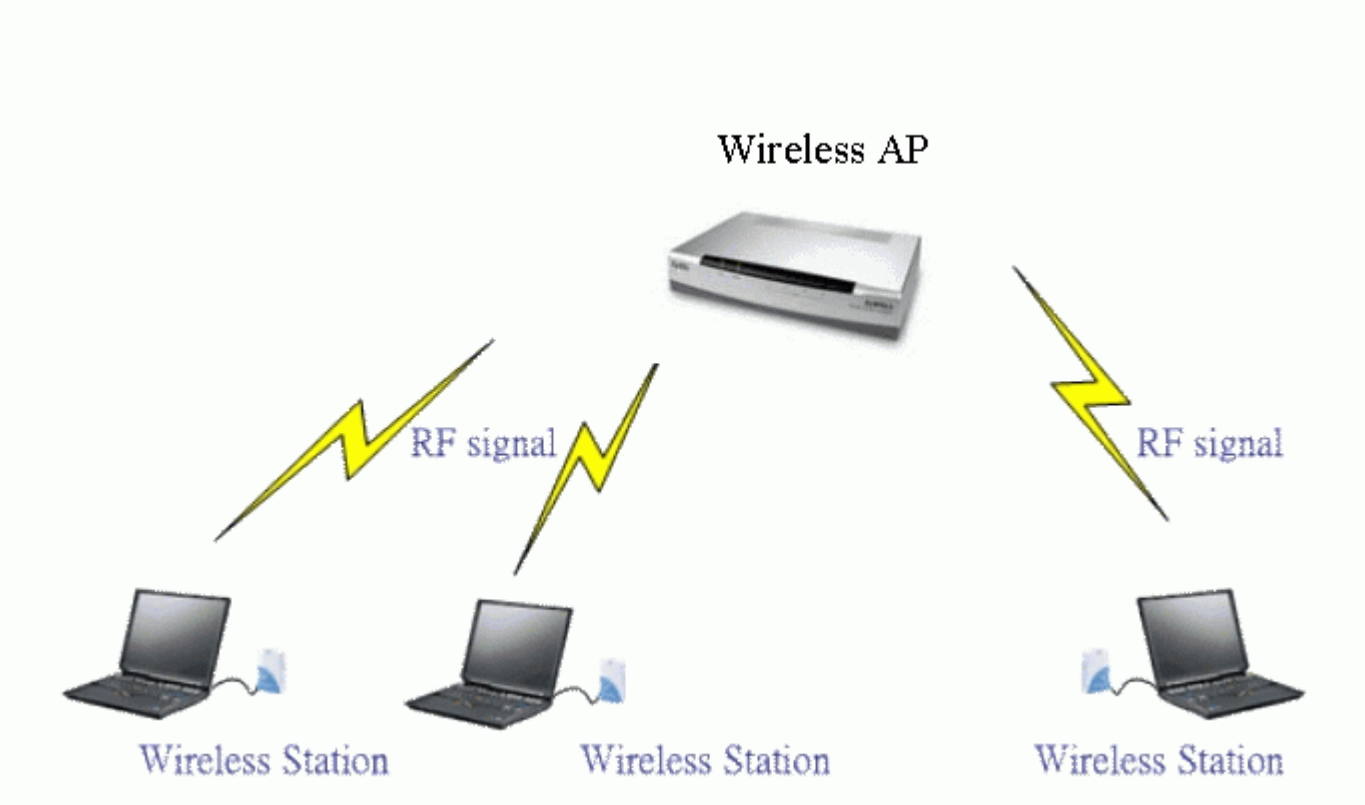
5. Finally, your video conversation is achieved.

WLAN Application Notes

Infrastructure Mode

1. What is Infrastructure mode?

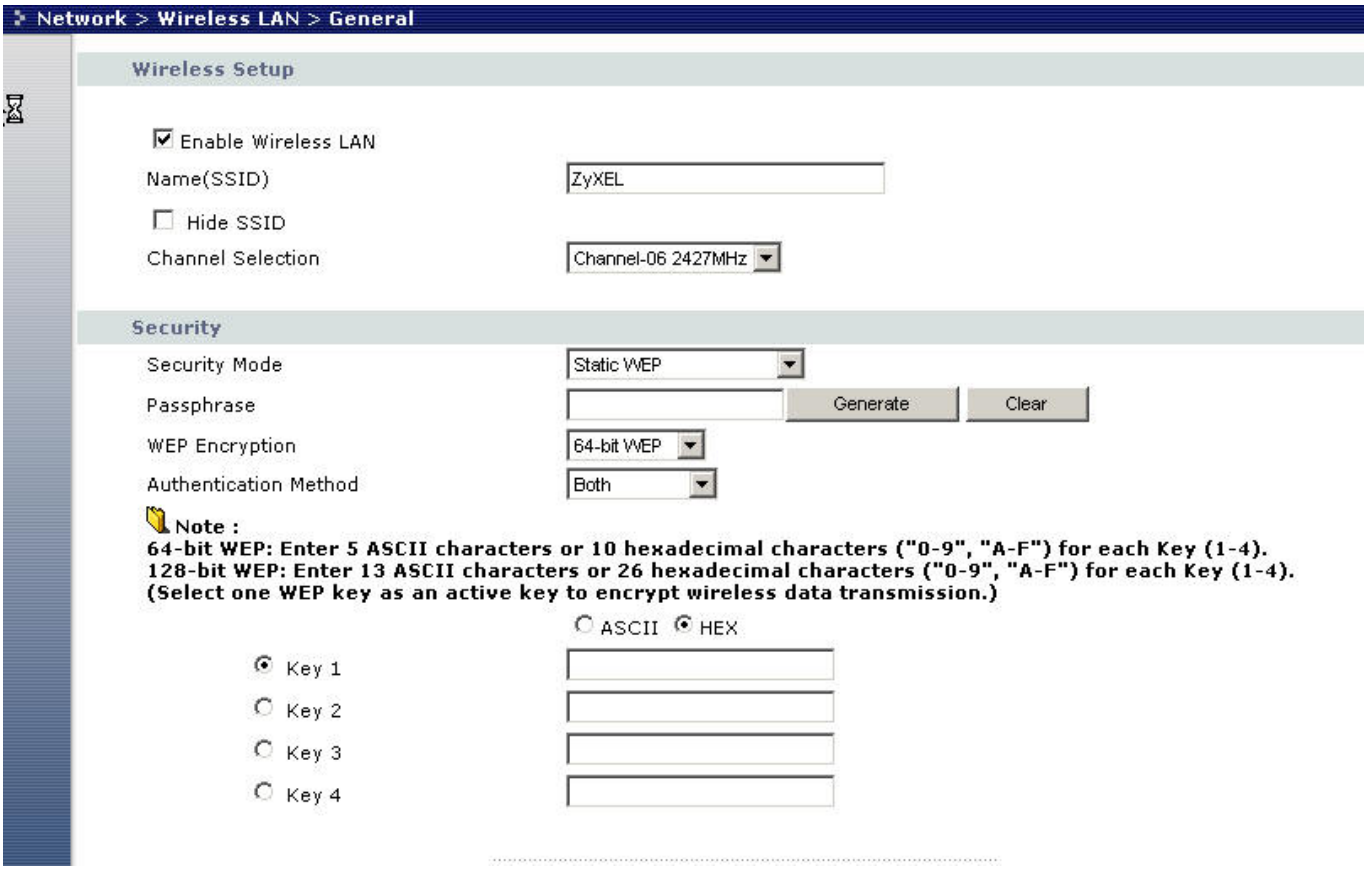
Infrastructure mode, sometimes referred to as Access Point mode, is an operating mode of an 802.11b/Wi-Fi client unit. In infrastructure mode, the client unit can associate with an 802.11b/Wi-Fi Access Point and communicate with other clients in infrastructure mode through that access point.



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

To configure Infrastructure mode of your P320W please follow the steps below.

a. From the web configurator main menu, go to Network > Wireless LAN



b. Configure the desired configuration on P320W. For each configurable parameter, what it is and how it function, please refer to the user's guide for detail or web help located on the page.

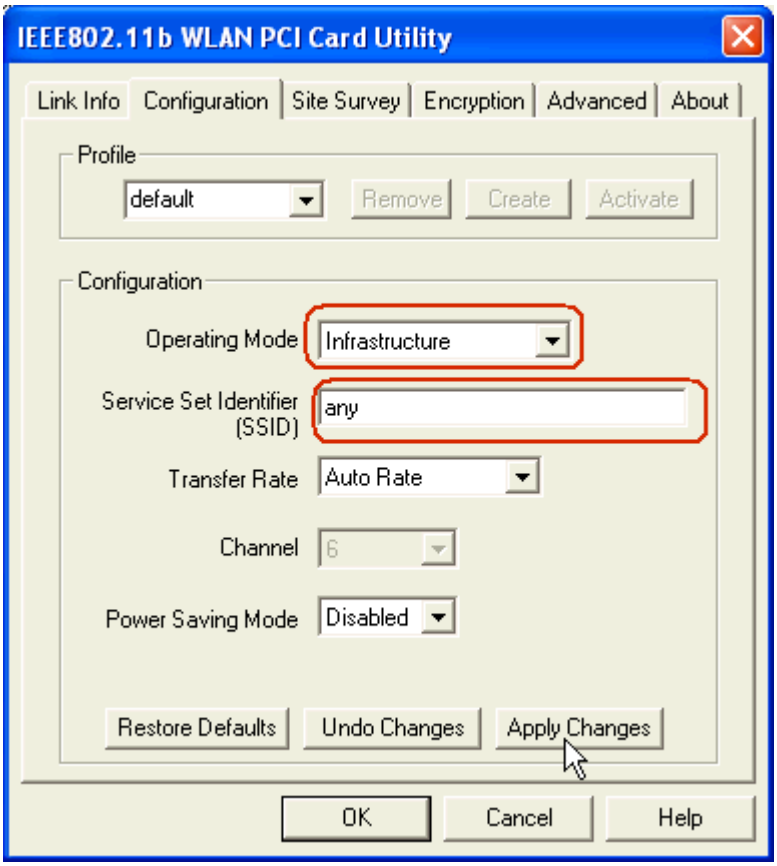
c. Finished.

3. Configuration Wireless Station to Infrastructure mode

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

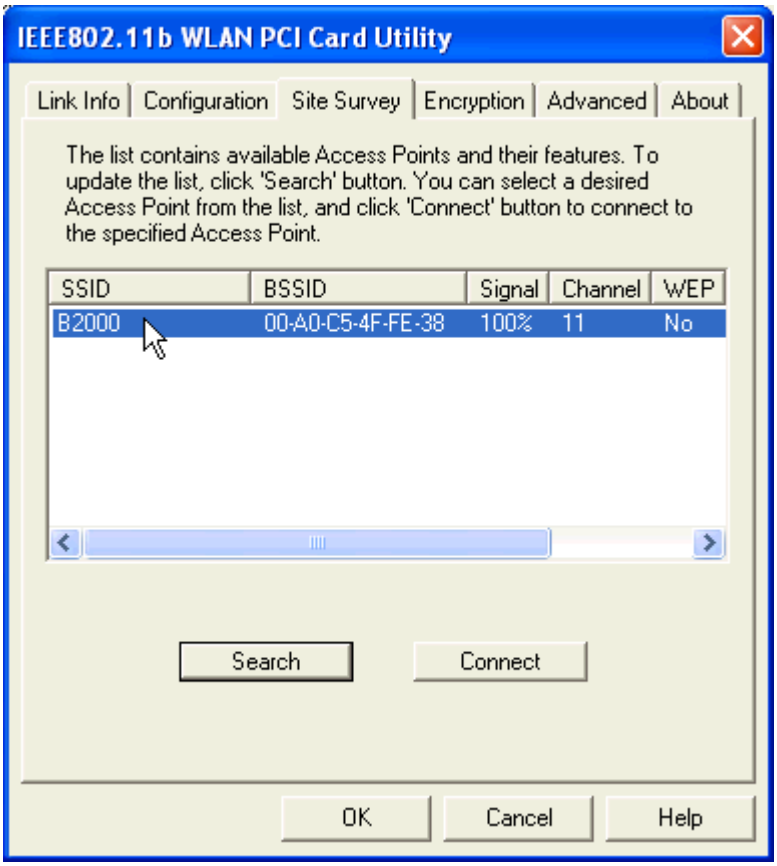
1. Double click on the utility icon in your windows task bar the utility will pop up on your windows screen.

2. Select configuration tab.

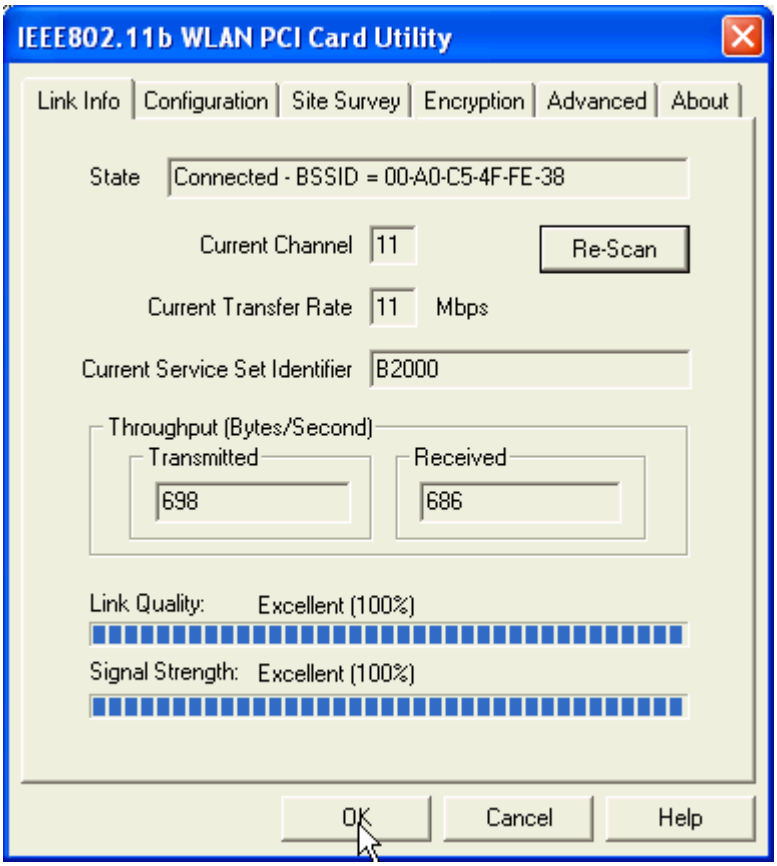


3. Select Infrastructure from the operation mode pull down menu, fill in an SSID or leave it as any if you wish to connect to any AP than press Apply Change to take effect.

4. Click on Site Survey tab, and press search all the available AP will be listed.



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

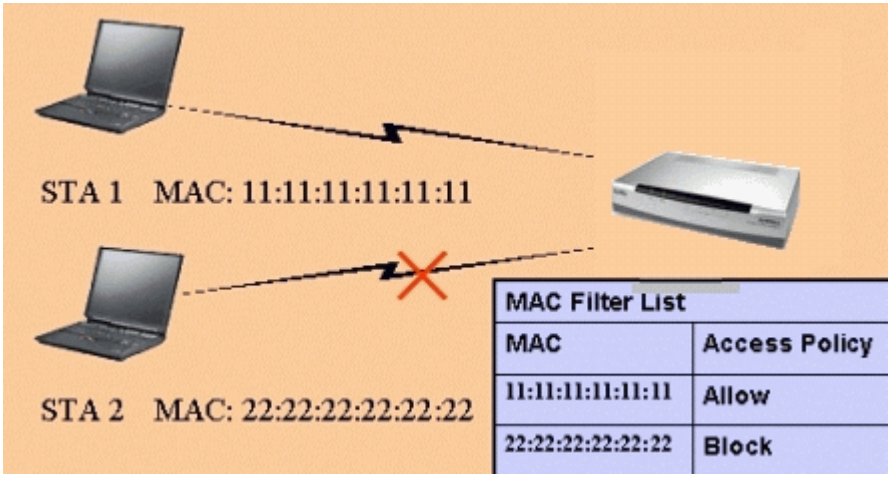


6. After the client have associated with the selected AP. The linked AP's channel, current linkup rate, SSID, link quality, and signal strength will show on the Link Info page. You now successfully associate with the selected AP with Infrastructure Mode.

Wireless MAC Address Filtering

1. MAC Filter Overview

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



2. ZyXEL MAC Filter Implementation

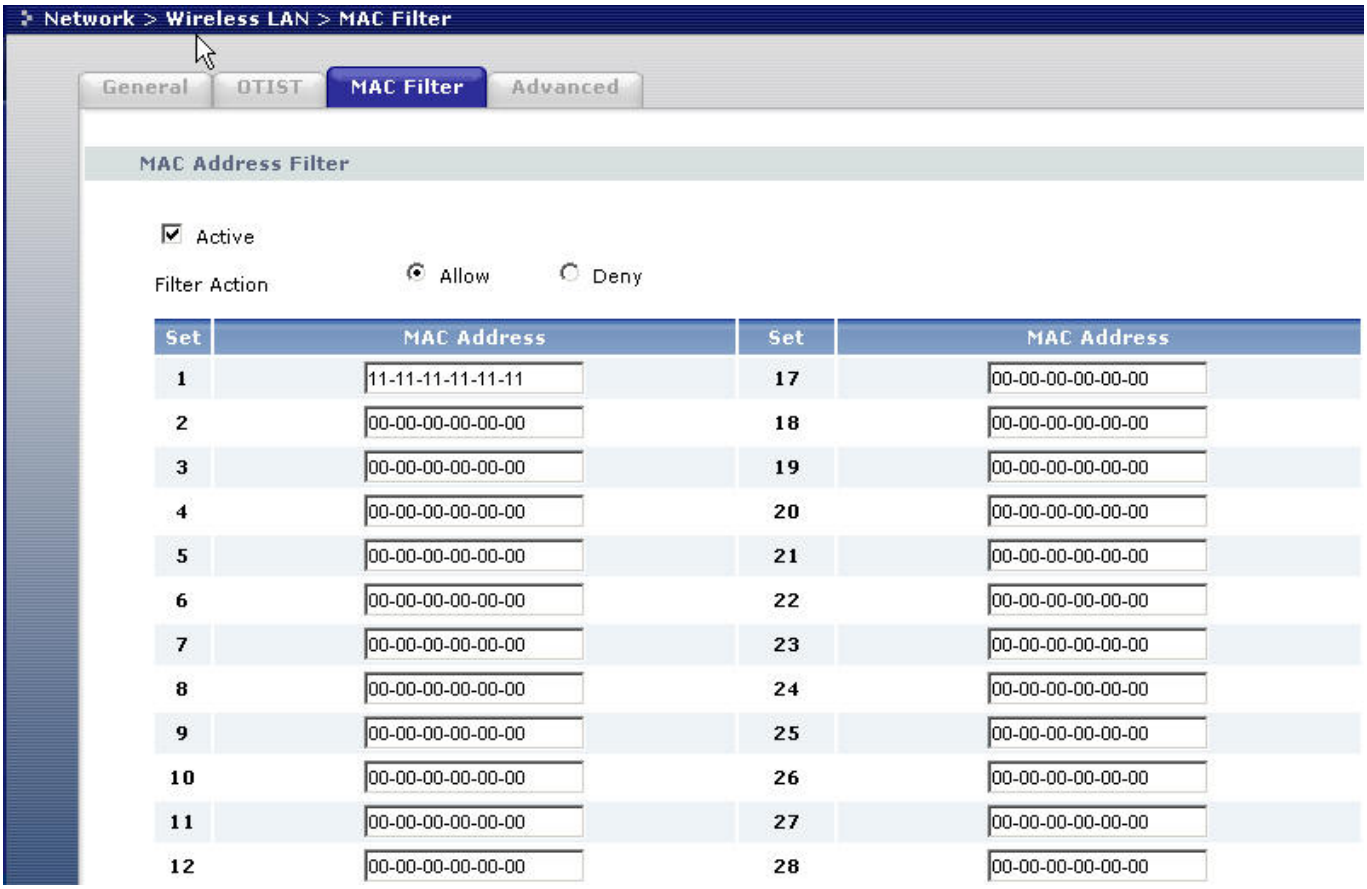
ZyXEL's MAC Filter Implementation allows users to define a list to allow or block association from STAs. The filter set allows users to input 32 entries in the list. If Allow Association is selected, all other STAs which are not on the list will be denied. Otherwise, if Deny Association is selected, all other STAs which are not on the list will be allowed for association. Users can choose either way to configure their filter rule.

3. Configure the WLAN MAC Filter

Before you configure the MAC filter, you need to know the MAC address of the client first. If not knowing what your MAC address is, please enter a command "**ipconfig /all**" after DOS prompt to get the MAC (physical) address of your wireless client.

By using WEB configuration, the MAC Address Filter configuration are as shown below.

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



WEP Configuration

1. Introduction

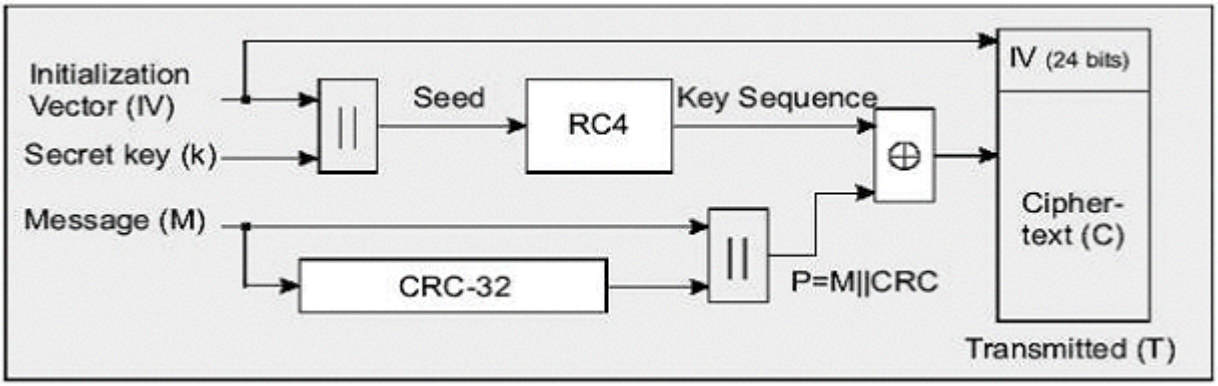
The 802.11 standard describes the communication that occurs in wireless LANs.

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

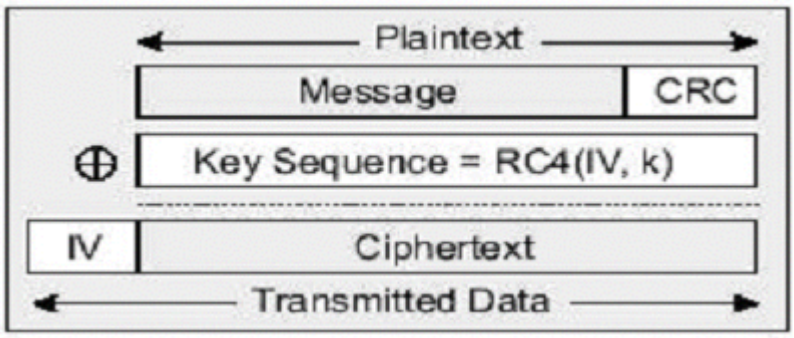
WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packages are not modified during the transition.

The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points APs.

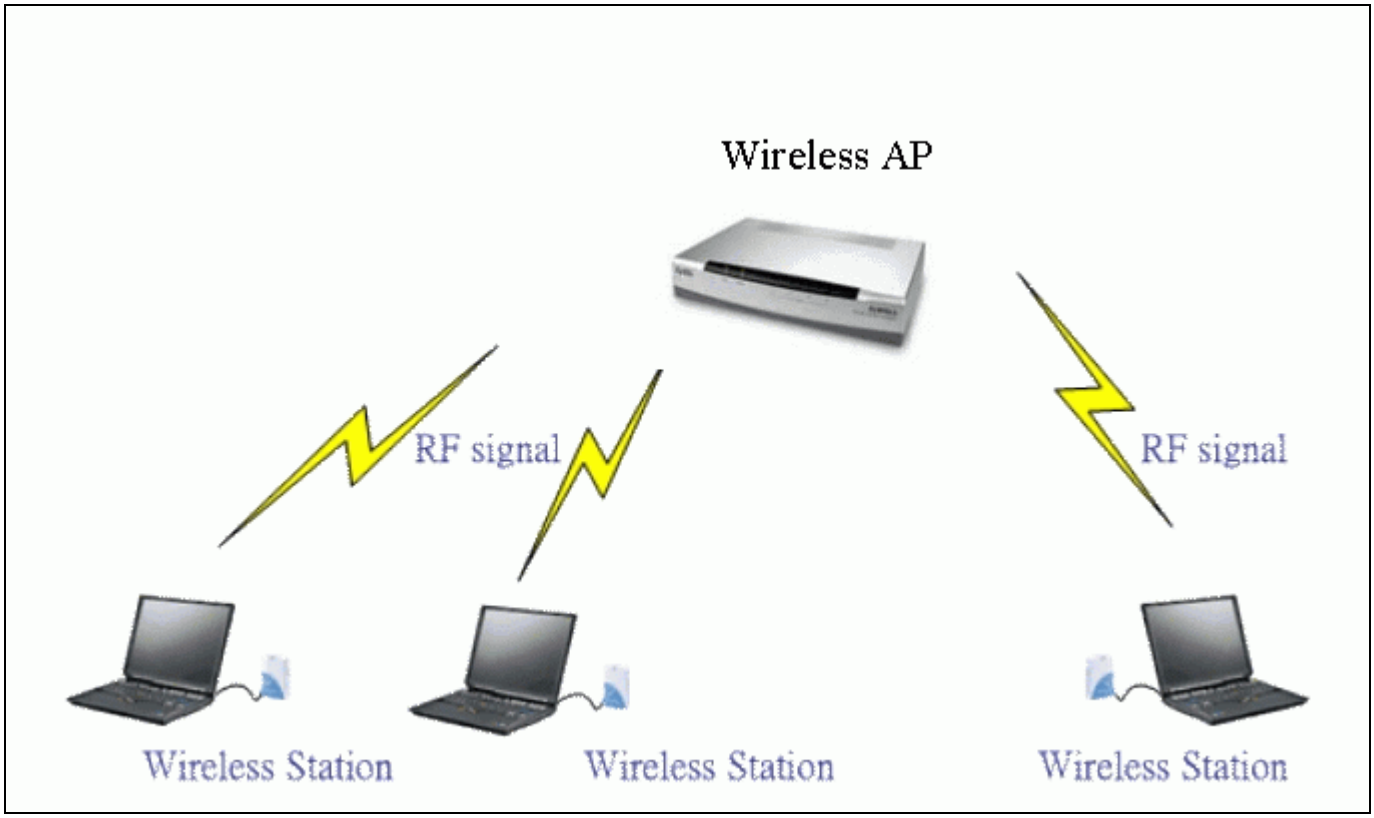
WEP employs the key encryption algorithm, Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG). The same key is used to encrypt and decrypt the data.



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



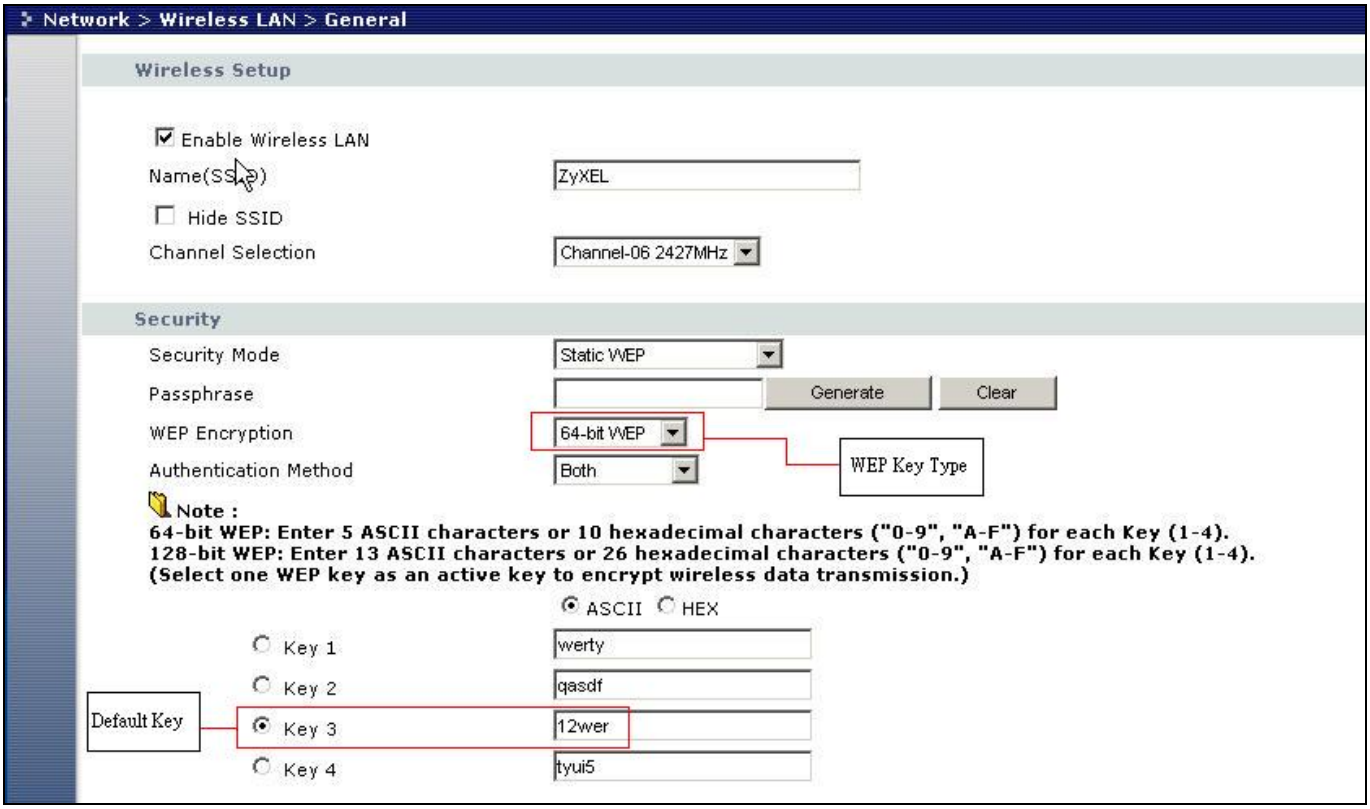
2. Setting up the Access Point



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

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

You can set up the Access Point in Web configurator



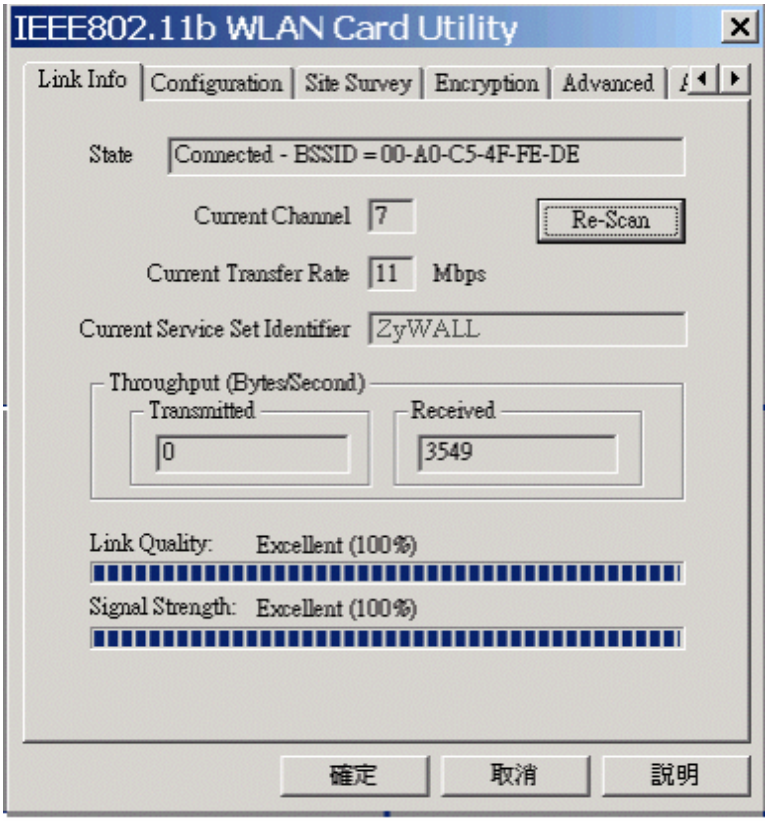
Key settings

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

3. Setting up the Station

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

The utility will pop up on your windows screen.



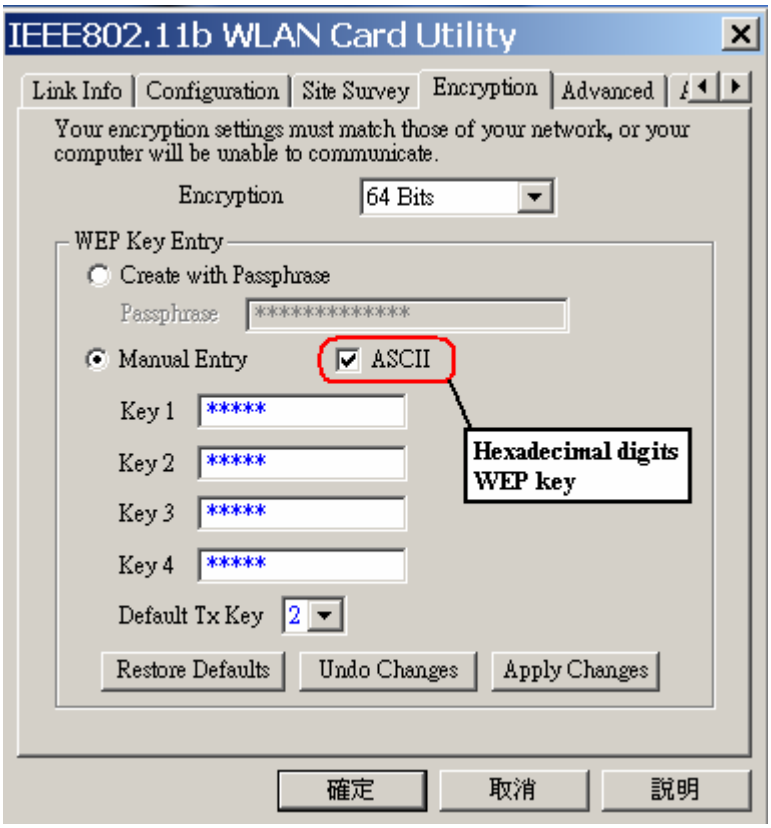
Note: If the utility icon doesn't exist in your task bar, click Start -> Programs -> IEEE802.11b WLAN Card -> IEEE802.11b WLAN Card.

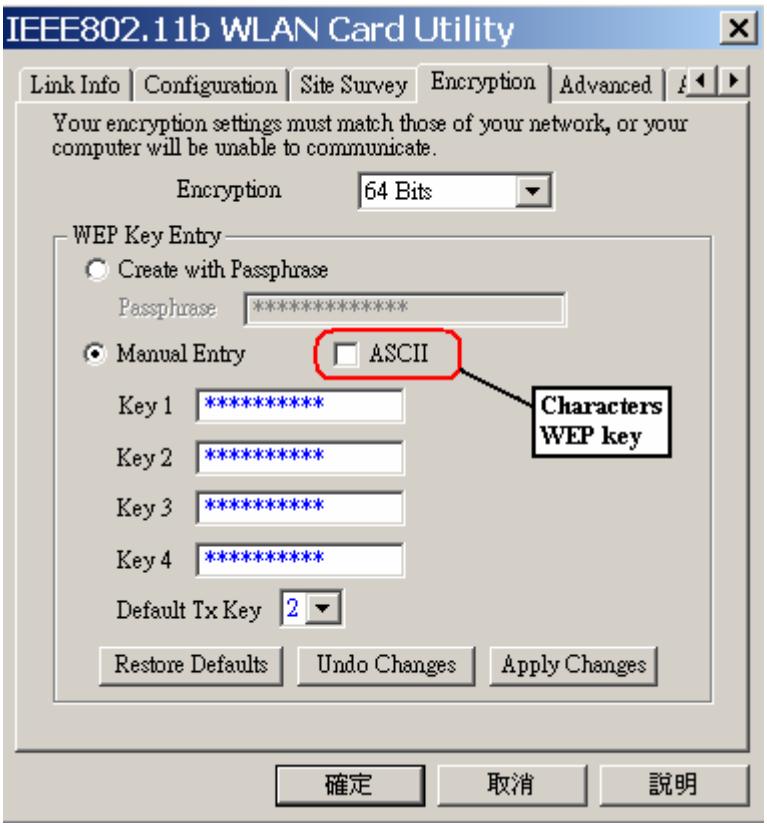
2. Select the 'Encryption' tab.

Select encryption type correspond with access point.

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

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





Key settings

The WEP Encryption type of station has to equal to the access point.
Check 'ASCII' field for characters WEP key or **uncheck 'ASCII'** field for Hexadecimal digits WEP key.
Hexadecimal digits don't need to proceed by '0x'.
For example,

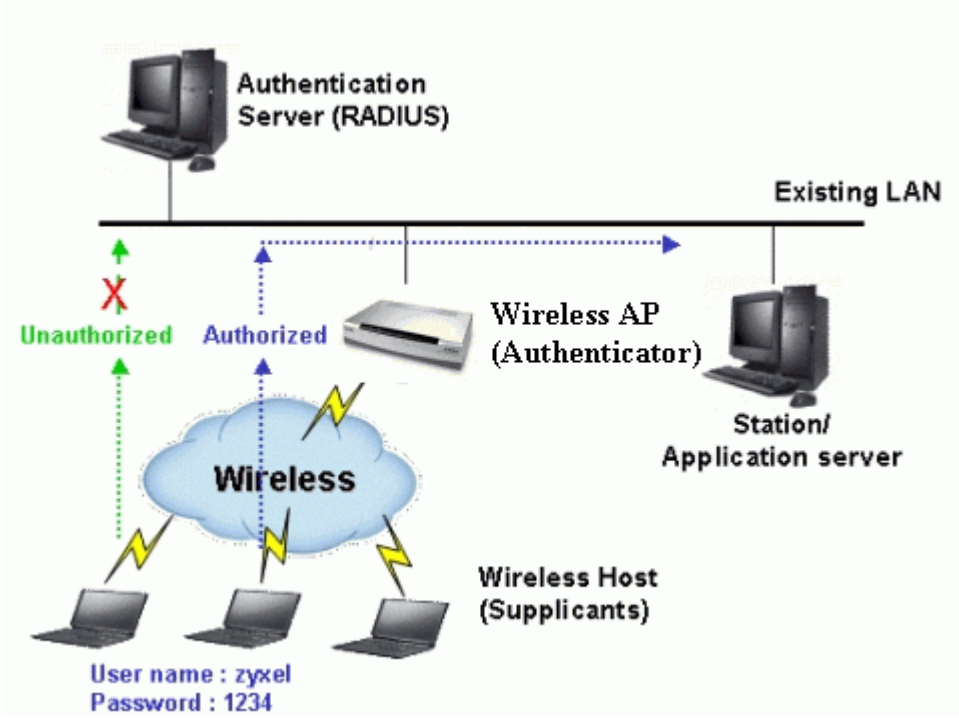
64-bits with characters WEP key:
Key1= 2e3f4
Key2= 5y7js
Key3= 24fg7
Key4= 98jui

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

IEEE 802.1x

1. IEEE 802.1x Introduction

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



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

1. Authenticator:

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

2. Supplicant:

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

3. Authentication Server:

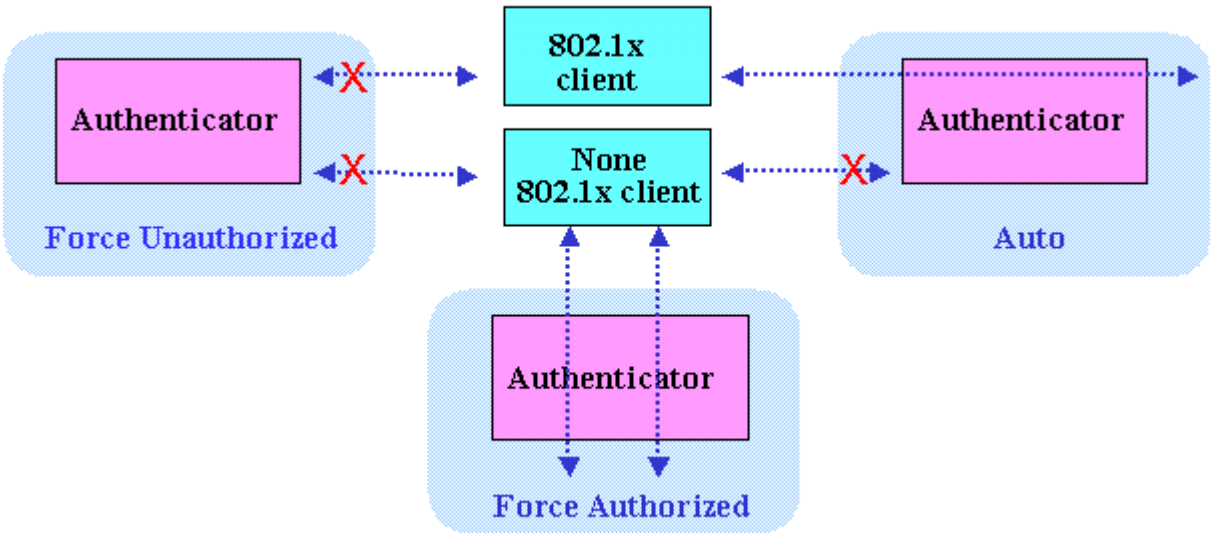
The device (i.e. RADIUS server) provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator. The authentication server performs the actual authentication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

Authentication Port State and Authentication Control

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

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

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



1. Force Authorized: Disables 802.1x and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default port control setting. While AP is setup as **Force Authorized**, Wireless client (supported 802.1x client or none-802.1x client) can always access the network.

2. Force Unauthorized: Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The authenticator cannot provide authentication services to the supplicants through the port. While AP is setup as **Force Unauthorized**, Wireless clients (supported 802.1x client or none-802.1x client) never have the access for the network.

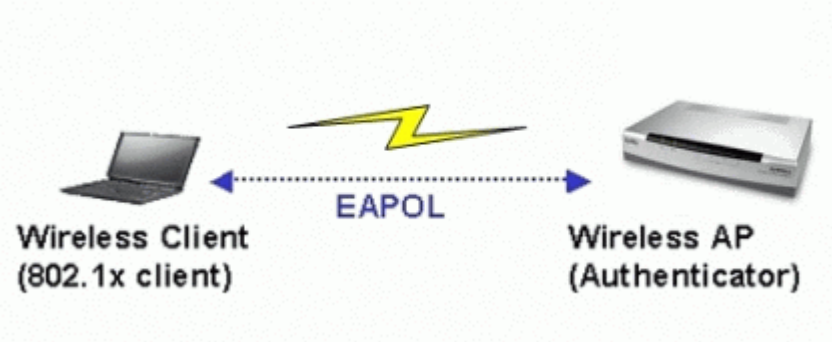
3. Auto: Enables 802.1x and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received requests the identity of the client and begins relaying authentication messages between supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the authenticator by using the client's MAC address. While AP is setup as **Auto**, only Wireless client supported 802.1x client can access the network.

Re-Authentication

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

EAPOL (Extensible Authentication Protocol over LAN)

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

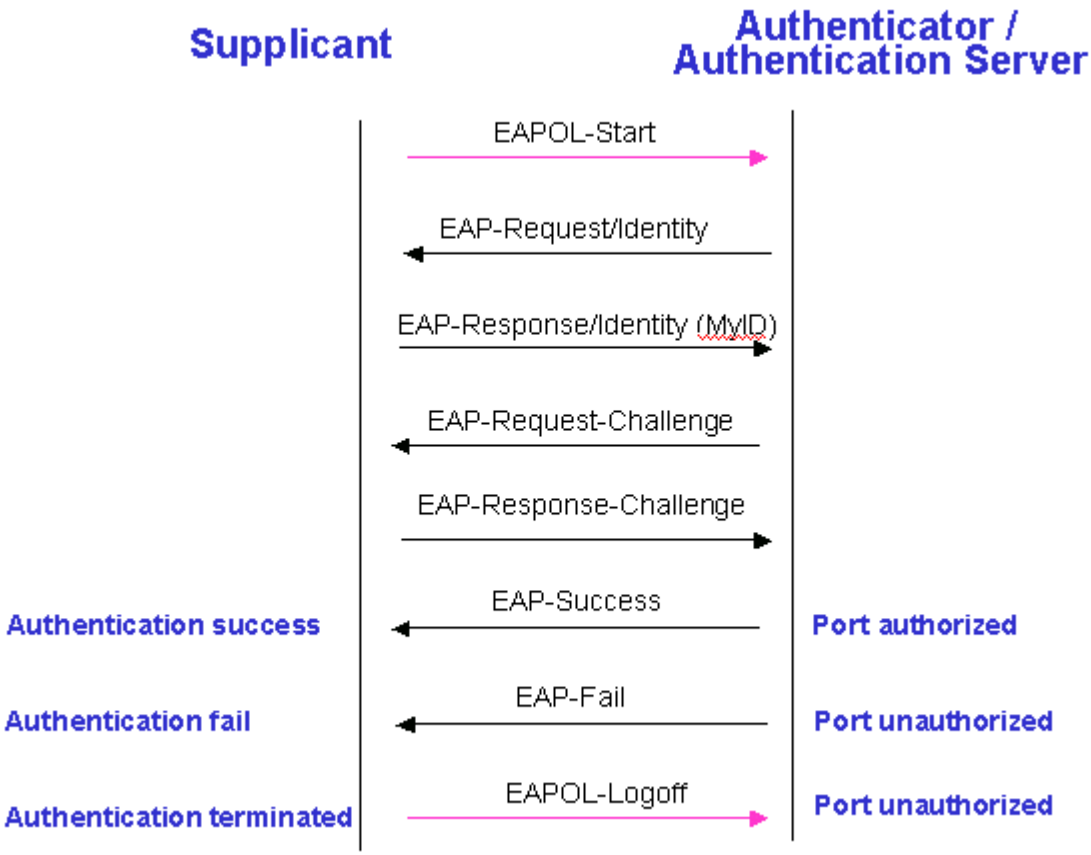


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When supplicant receive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

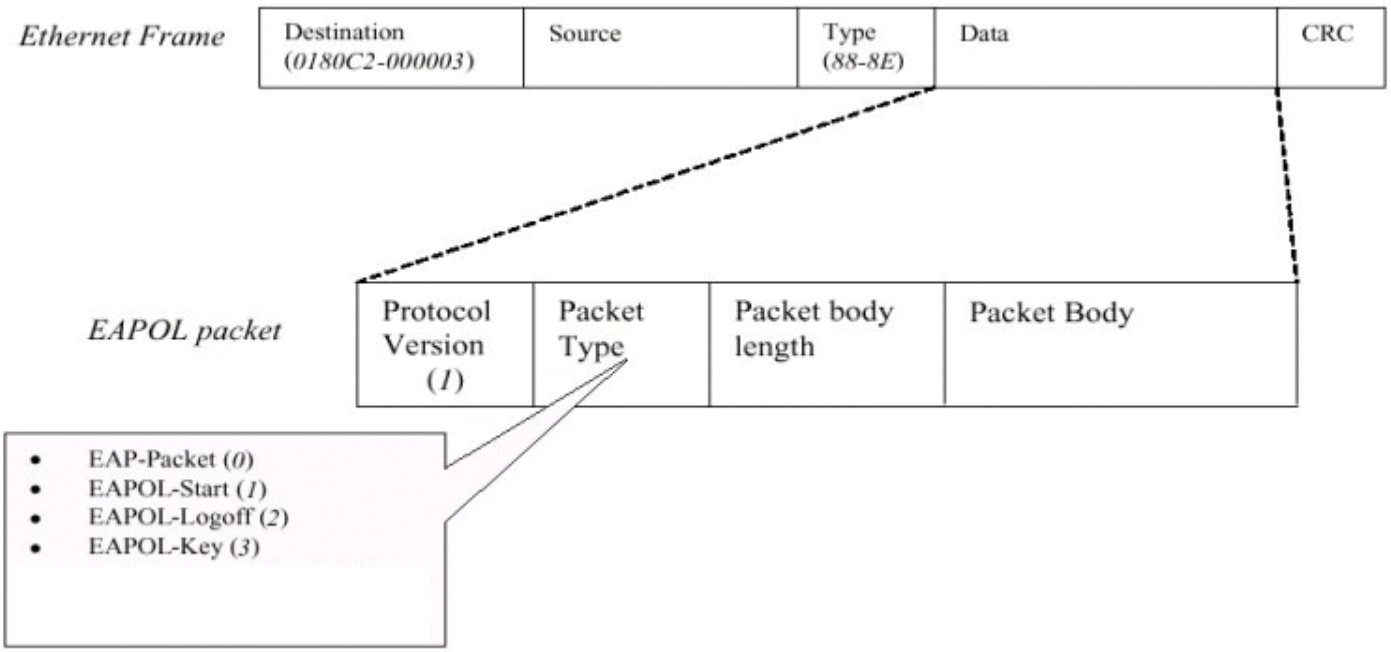
EAPOL Exchange between 802.1x Authenticator and Supplicant

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

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



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



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

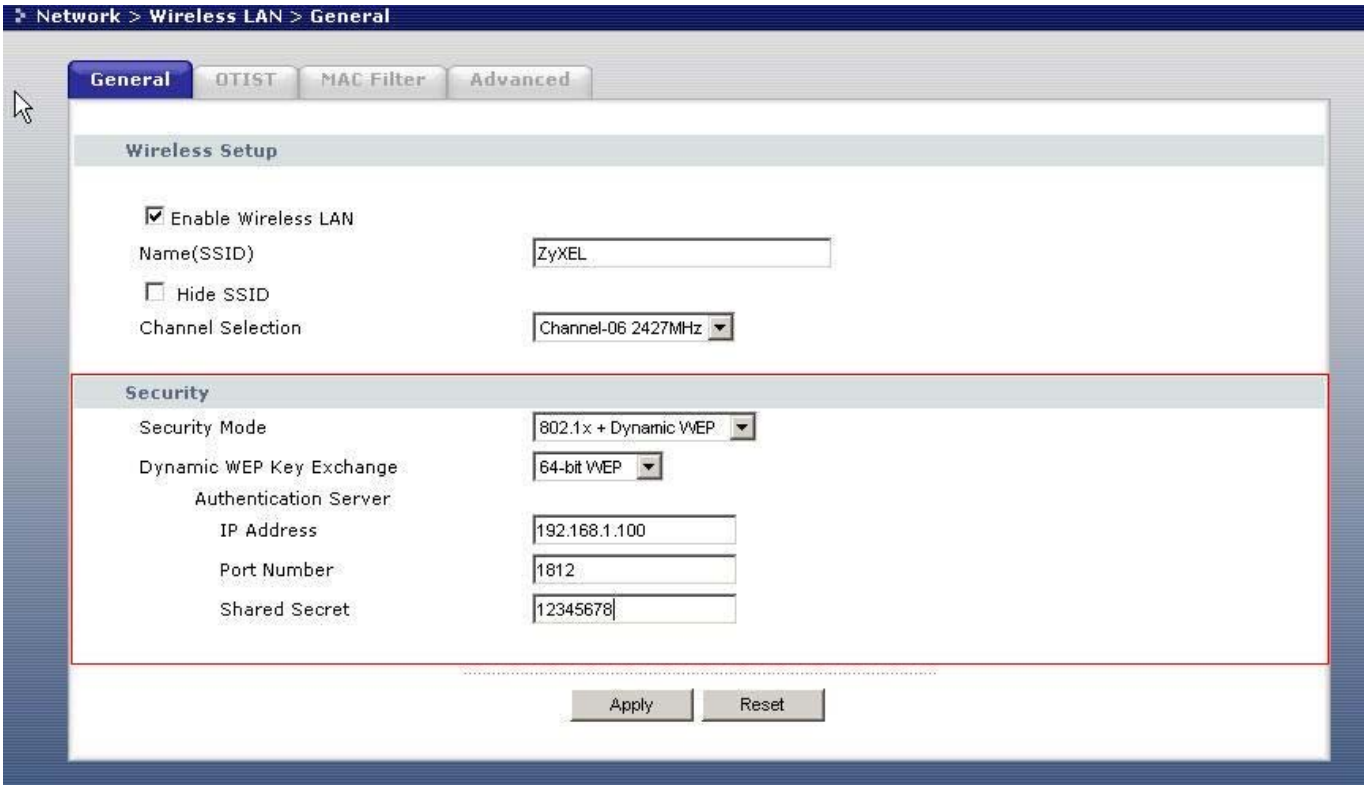
IEEE 802.1x Configuration in ZyXEL Wireless Access Point

- ***Enable 802.1x in AP***

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

Using WEB Configuration,

1. From the Web Configurator main menu, go to Network > Wireless LAN > General
2. Select **802.1x+Dynamic WEP** to enable 802.1x authentication function.
3. Click **Apply** to make your setting work.

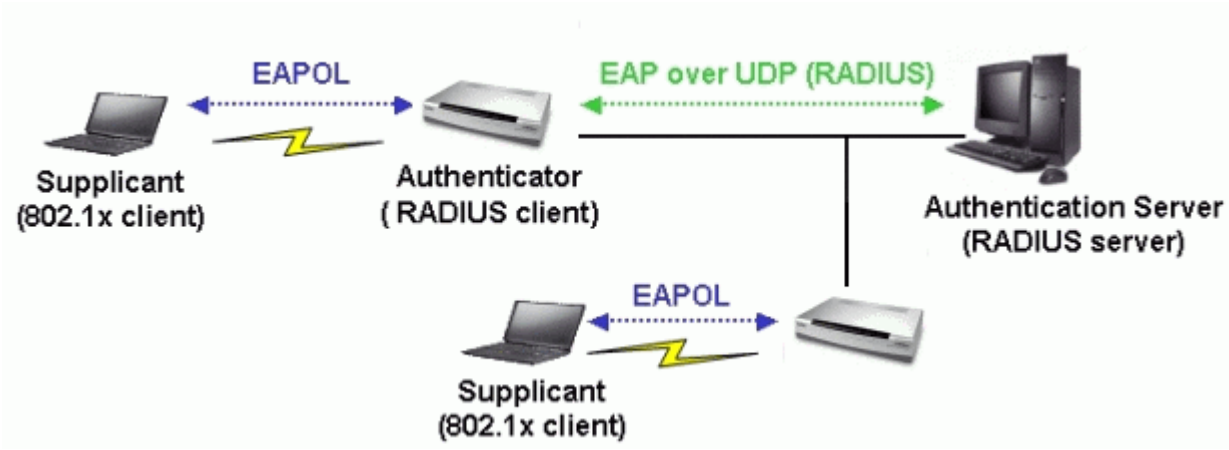


After 802.1x authentication function is enabled, you have to setup the authentication server, you need to specify the location and port of an **external RADIUS authentication server**.

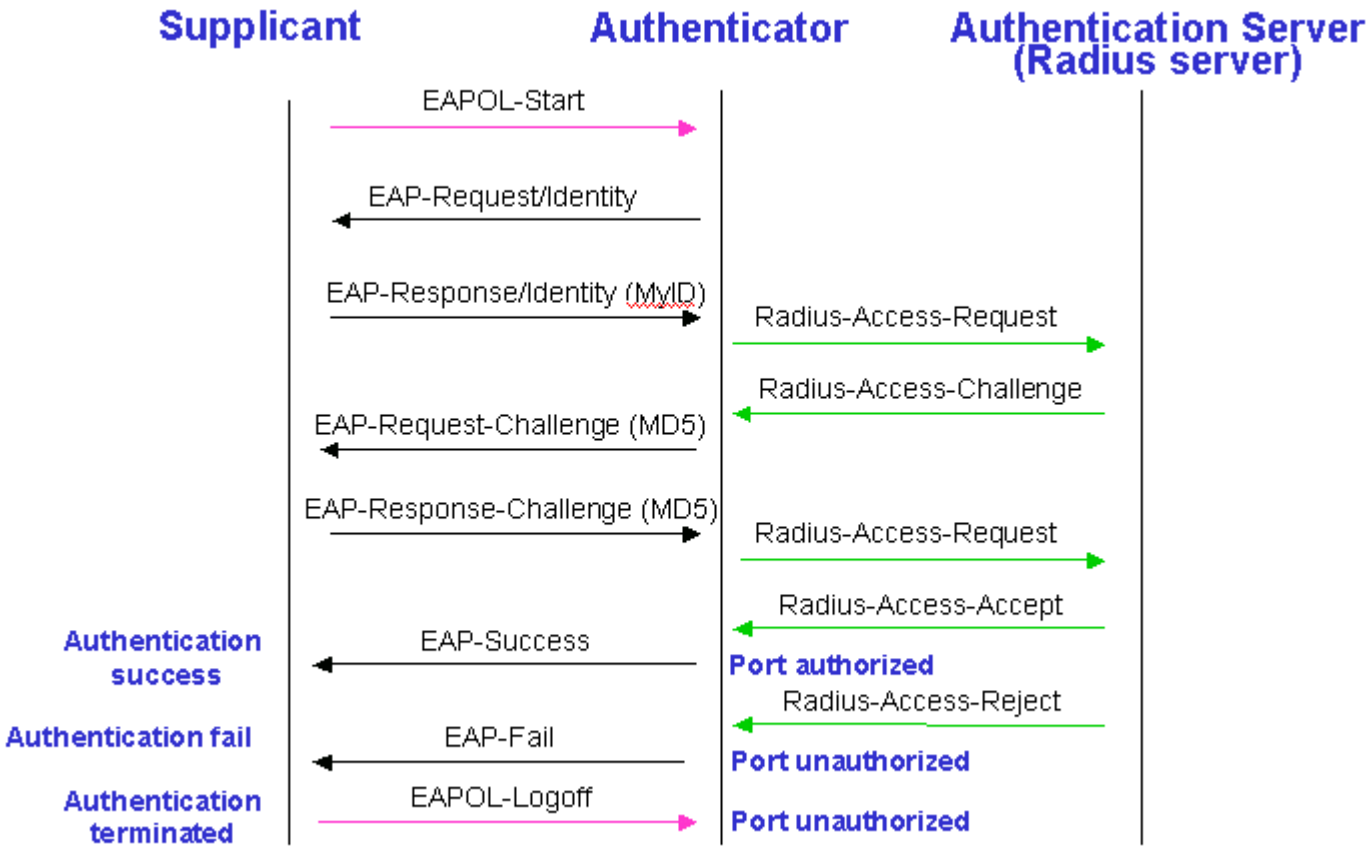
- ***Using External RADIUS Authentication Server***

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The wireless AP is the client and the server is the RADIUS server.

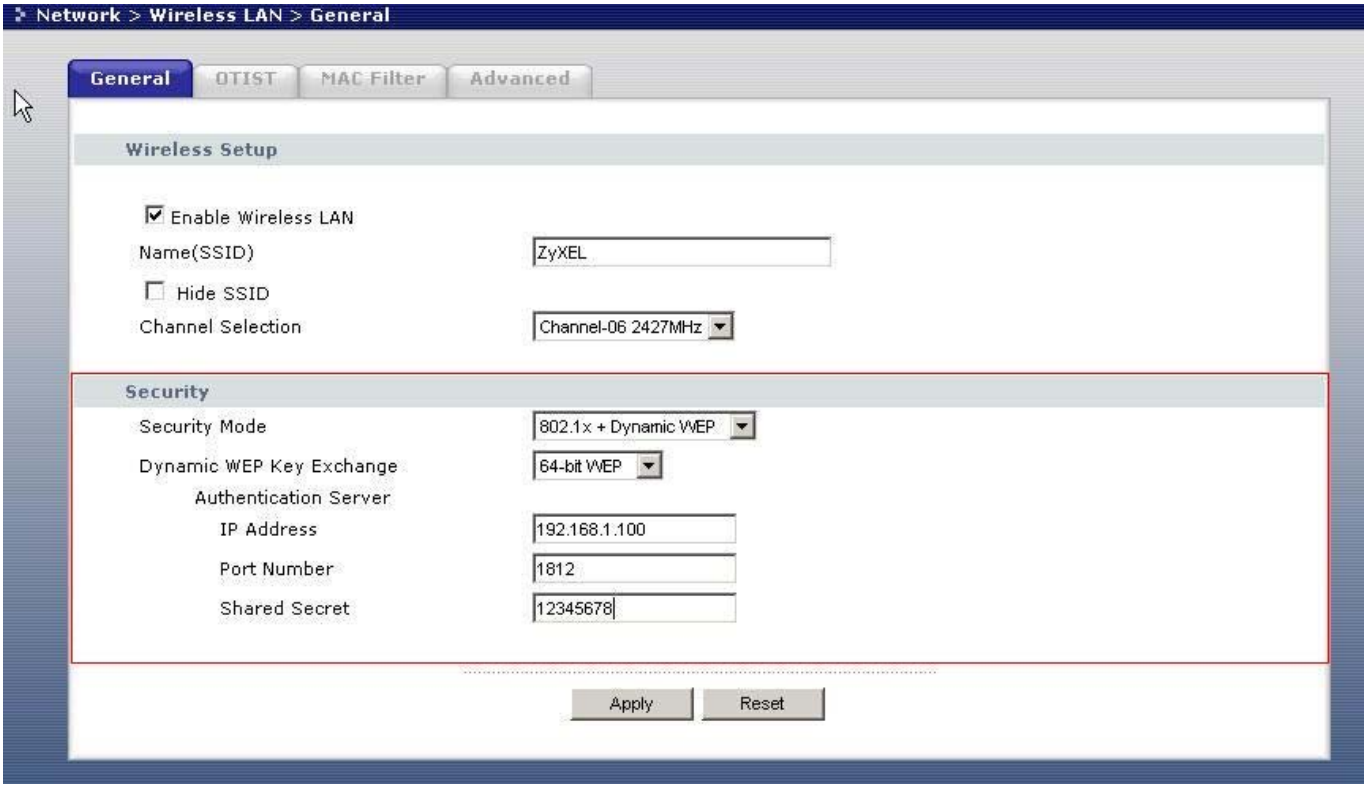
The authenticator includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the authenticator receives EAPOL frames and relays them to the authentication server, the Ethernet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



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



By using WEB Configurator, set up Authentication server address, port number (1812) and shared secret as below



Site Survey

1. Introduction

What is Site Survey?

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

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

2. 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 a blueprint. This is for you to mark and take record on.

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

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

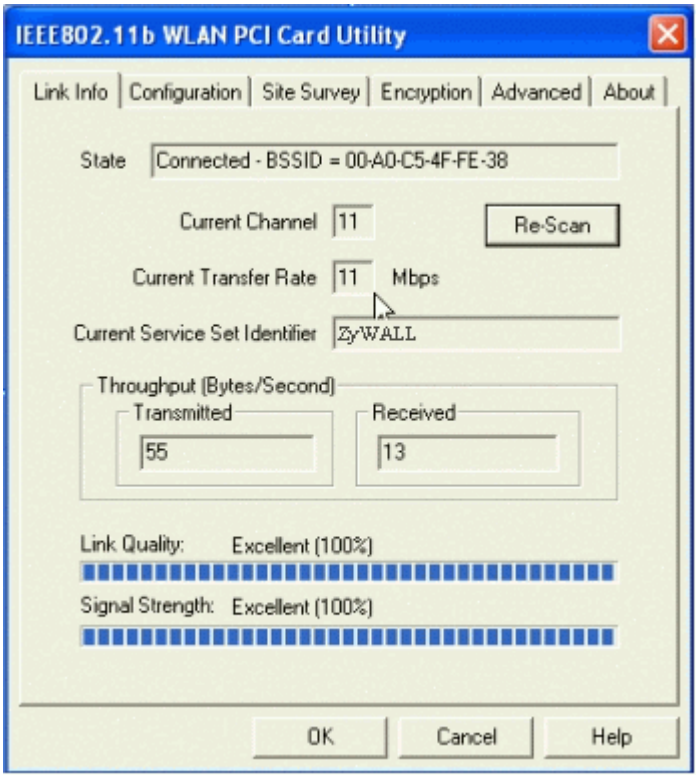
4. Determine the preliminary access point location on the facility diagram base on the service area needed, obstacles, and power wall jack considerations.

3. Survey on Site

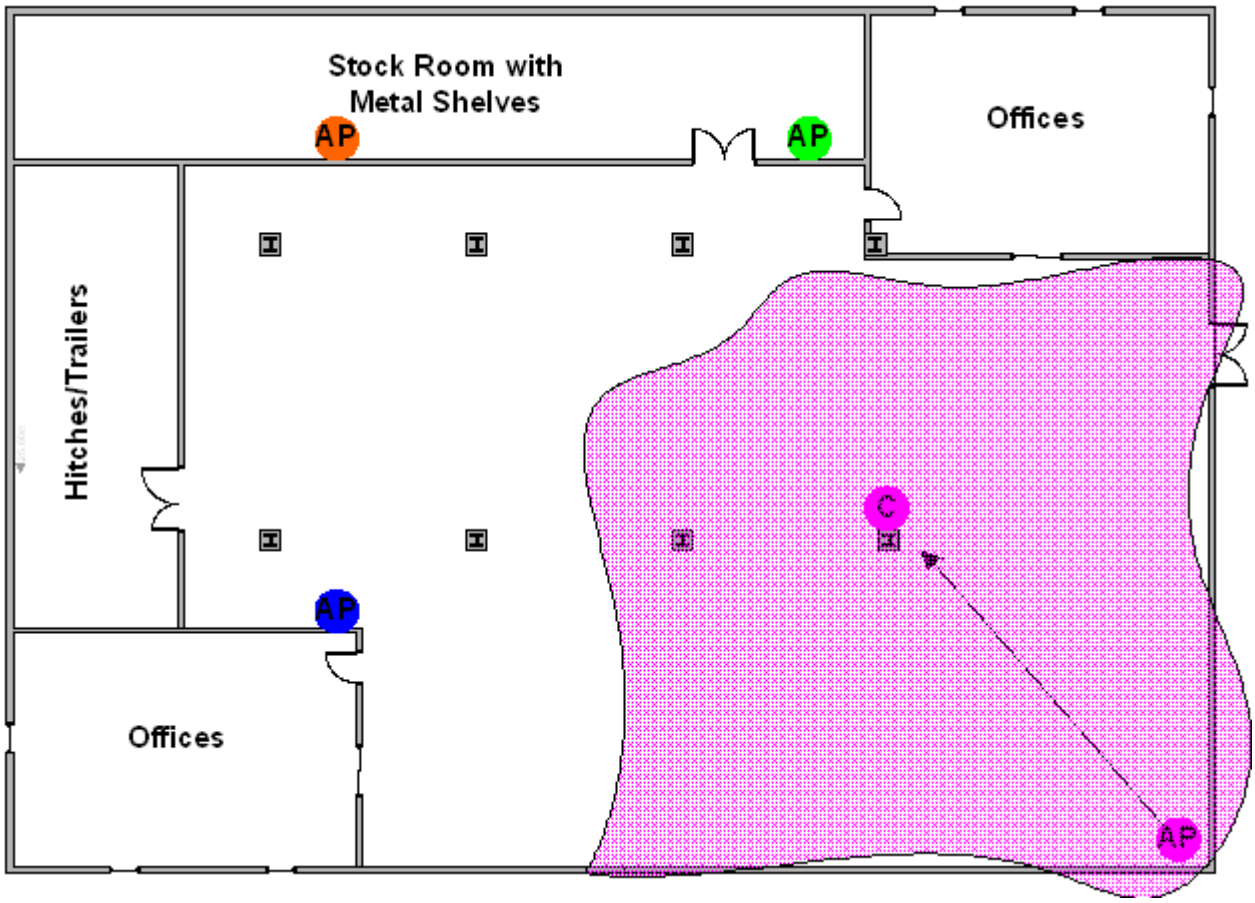
1. With the diagram with all information you gathered in the preparation phase. Now you are ready to make the survey.

2. Install an access point at the preliminary location.

3. User a notebook with wireless client installed and run it's utility. A utility will provide information such as connection speed, current used channel, associated rate, link quality, signal strength and etc information as shown in utility below.



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

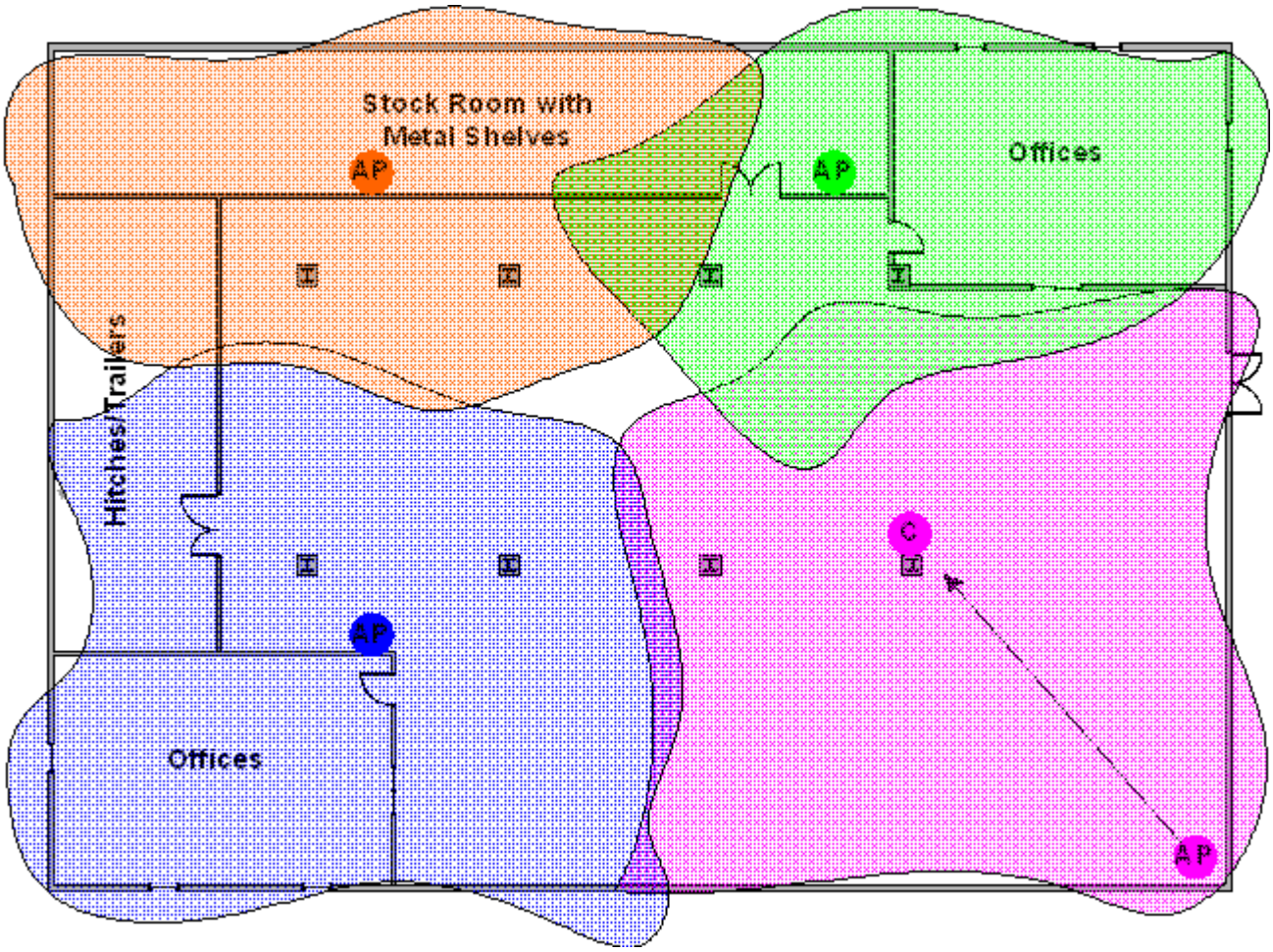


5. When you reach the farthest point of connection mark the spot. Now you move the access point to this new spot as have already determine the farthest point of the access point installation spot if wireless service is required from corner of the room.

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

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

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



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

FAQ

Product FAQ

What is the P320W 802.11g Wireless Firewall Router?

The P320W 802.11g Wireless Firewall Router integrated with wireless LAN, Access Point, firewall and 4-port switch is designed for residential and home users. The P320W provides a robust Firewall to protect

your network. Prestige's design helps users to save expenses, minimize maintenance, and simultaneously provide a high quality networking environment.

The P320W is a robust solution complete with everything needed for providing Internet access to multiple workstations through your cable or ADSL modem. The router equipped with 1 10/100Mbps Ethernet WAN port and 4 10/100Mbps Ethernet LAN port.

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

Will the P320W work with my Internet connection?

The P320W is designed to be compatible with cable and ADSL modems. Most external Cable and ADSL modems use an Ethernet port to connect to your computer so the Prestige is placed in the line between the computer and the External modem. As long as your Internet Access device has an Ethernet port, you can use the Prestige. Besides, if your ISP supports PPPoE you can also use the Prestige, because PPPoE had been supported in the Prestige.

What do I need to use the Prestige?

You need an ADSL modem or cable modem with an Ethernet port to use the Prestige. The Prestige has two Ethernet ports: LAN port and WAN port. You should connect the computer to the LAN port and connect the external modem to the WAN port.

What is PPPoE?

PPPoE stands for **P**oint-to-**P**oint **P**rotocol **O**ver **E**thernet that is an IETF draft standard specifying how a computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to the high-speed data networks via a familiar PPP dialer such as 'Dial-Up Networking' user interface. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management. There are some service providers running of PPPoE today. Before configuring PPPoE in the Prestige, please make sure your ISP supports PPPoE.

Does the Prestige support PPPoE?

Yes. The Prestige supports PPPoE.

How do I know I am using PPPoE?

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

Why does my provider use PPPoE?

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

Which Internet Applications can I use with the Prestige?

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

How can I configure the Prestige?

Web browser- web server embedded for easy configurations

What network interface does the Prestige support?

The Prestige supports 4*10/100M Ethernet to connect to the computer and 10M Ethernet to connect to the external cable or ADSL modem..

What can we do with Prestige?

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

Does Prestige support dynamic IP addressing?

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

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

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

How does e-mail work through the Prestige?

It depends on what kind of IP you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through Prestige Internet Access Sharing Router using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access right.

If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address.

Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through Prestige Internet Access Sharing Router using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access right.

What is the main difference between WinGate and the Prestige?

1. WinGate is a software only solution that needs to be installed in a dedicated Windows 95 PC based server. The total cost and complexity are many times over ATI’s product. The Prestige Internet Access Sharing Router is a plug-n-play internet appliance.
2. WinGate requires all TCP/IP applications such as Netscape Navigator to be reconfigured to have the dedicated server as a proxy. The Prestige Internet Access Sharing Router does not require users to reconfigure any software at all.
3. The Prestige Internet Access Sharing Router uses Network Address Translation (NAT) scheme, which supports all TCP/UDP ports. WinGate only supports limited number of ports, such as http(80), ftp(21), telnet(23), and pop3(110).
4. WinGate works as a proxy, while the Prestige Internet Access Sharing Router works as a gateway. The gateway approach is more efficient than the proxy during the processing of TCP/IP commands. As a result, the Prestige Internet Access Sharing Router achieves 10% to 20% higher performance than that of software solutions such as WinGate.

5. The Prestige Internet Access Sharing Router uses Solid State Disk technology. There are no moving parts in the product. It is much more reliable than any hard disk based system, such as the one for WinGate.

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

Yes, it is possible because Prestige delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured in Network>NAT>Port Forwarding

What DHCP capability does the Prestige support?

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

What network interface does the new Prestige series support?

The Prestige series support 4*10/100M Ethernet LAN port to connect to the computer on LAN and 1*10/100M Ethernet to connect to the external cable or ADSL modem on WAN.

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

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

How fast can the data go?

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

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

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

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

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

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

How fast can they go? In a perfect world (or lab) they can receive data at speeds up to 30 Mbps. In the real world, with cost conscious cable companies running the systems, the speed will probably fall to about 1.5 Mbps.

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

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

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

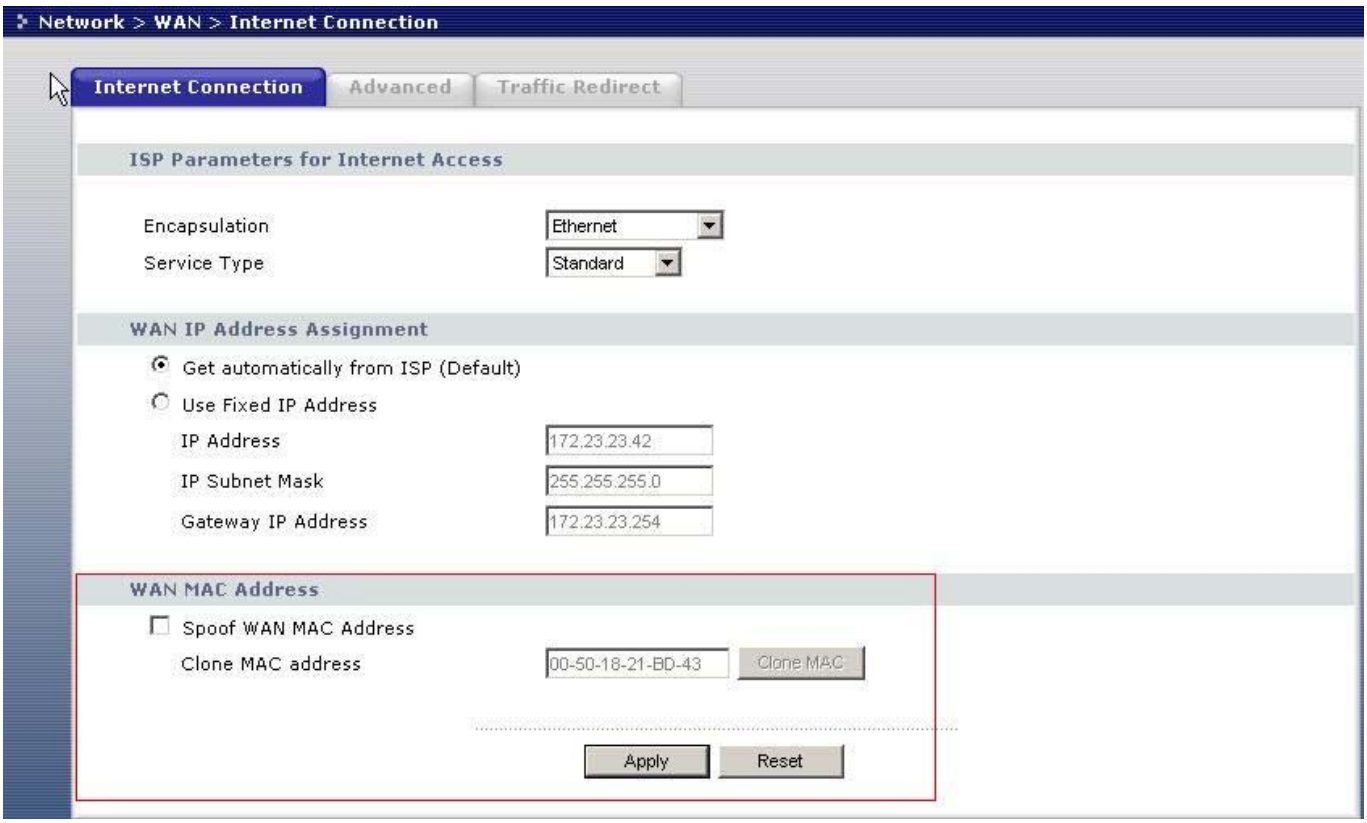
If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for the authentication. So, if a new network card is used or

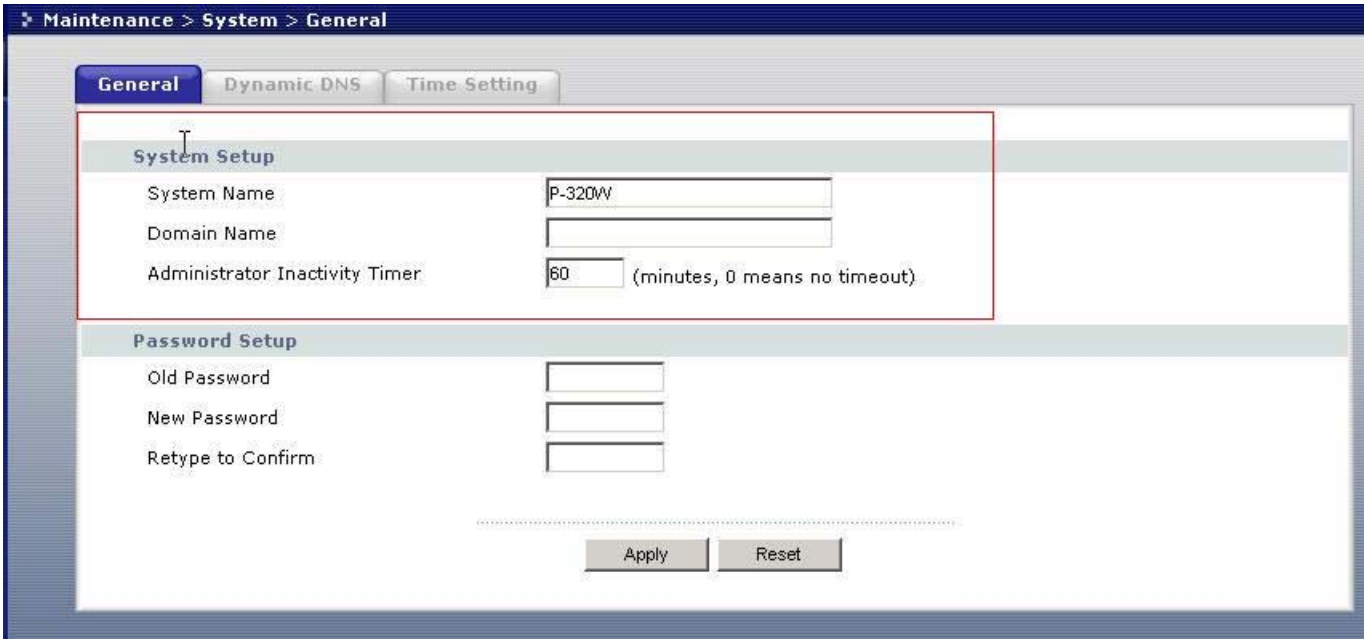
the Prestige is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP.

The Prestige supports to clone the MAC from the first PC the ISP installed to be its WAN MAC. To clone the MAC from the PC you need to enter that PC's IP in Network > WAN > Internet Connection. Once the MAC is received by the Prestige, the WAN MAC will be updated and used for the ISP's authentication.



2. Your ISP checks the 'Host Name'

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



What is BOOTP/DHCP

BOOTP stands for Bootstrap Protocol. DHCP stands for Dynamic Host Configuration Protocol. Both are mechanisms to dynamically assign an IP address for a TCP/IP client by the server. In this case, the Prestige Internet Access Sharing Router is a BOOTP/DHCP server. Win95 and WinNT clients use DHCP to request an internal IP address, while WFW and WinSock clients use BOOTP. TCP/IP clients may specify their own IP or utilize BOOTP/DHCP to request an IP address.

What is DDNS

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

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

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

When do I need DDNS service?

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

What DDNS servers does the Prestige support?

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

What is DDNS wildcard?

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

Does the Prestige support DDNS wildcard?

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

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

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

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

Built-in firewall function is supported in P320W. When a session is initiated from a user located in P320W's LAN network, incoming traffic will be allowed by Stateful Inspection mechanism. However, if the session is initiated from WAN side and there is no related access rule for the incoming traffic, the

traffic will be blocked by P320W. To help users get rid of the problem and configuration tasks, P320W will create firewall policy automatically to allow incoming traffic if NAT is enabled in the P320Ws.

Firewall FAQ

What is a network firewall?

A firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. The firewall can be thought of two mechanisms. One to block the traffic, and the other to permit traffic.

What makes P320W secure?

The P320W is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND attack, IP Spoofing, etc. It also uses stateful packet inspection to determine if an inbound connection is allowed through the firewall to the private LAN. The P320W supports Network Address Translation (NAT), which translates the private local addresses to one public address. This adds a level of security since the clients on the private LAN are invisible to the Internet.

What are the basic types of firewalls?

Conceptually, there are three types of firewalls:

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

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

Application-level Firewalls generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform logging and auditing of traffic passing through them. A proxy server is an application gateway or circuit-level gateway that runs on top of general operating system such

as UNIX or Windows NT. It hides valuable data by requiring users to communicate with secure systems by mean of a proxy. A key drawback of this device is performance.

Stateful Inspection Firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also 'inspect' the session data to assure the integrity of the connection and to adapt to dynamic protocols. The flexible nature of Stateful Inspection firewalls generally provides the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support.

What kind of firewall is the P320W?

1. The P320W's firewall inspects packets 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 P320W's firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
3. The P320W's firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
4. The P320W's firewall is fast. It uses a hashing function to search the matched session cache instead of going through every individual rule for a packet.

Why do you need a firewall when your router has packet filtering and NAT built-in?

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

What is Denials of Service (DoS) attack?

Denial of Service (DoS) attacks is aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

There are four types of DoS attacks:

1. Those that exploits bugs in a TCP/IP implementation such as Ping of Death and Teardrop.

2. Those that exploits weaknesses in the TCP/IP specification such as SYN Flood and LAND Attacks.
3. Brute-force attacks that flood a network with useless data such as Smurf attack.
4. IP Spoofing

What is Ping of Death attack?

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

What is Teardrop attack?

Teardrop attack exploits weakness in the reassemble of the IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original packet except that it contains an offset field. The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

What is SYN Flood attack?

SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response, while the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set a relatively long intervals) terminates the TCP three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

What is LAND attack?

In a LAN attack, hackers flood SYN packets to the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

What is Brute-force attack?

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

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

What is IP Spoofing attack?

Many DoS attacks also use IP Spoofing as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP Spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall.

Wireless FAQ

What is a Wireless LAN?

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

What are the advantages of Wireless LANs?

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

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

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

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

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

What are the disadvantages of Wireless LANs?

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

Where can you find wireless 802.11 networks?

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

What is an Access Point?

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

What is IEEE 802.11?

The IEEE 802.11 is a wireless LAN industry standard, and the objective of IEEE 802.11 is to make sure that different manufactures' wireless LAN devices can communicate to each other.802.11 provides 1 or 2 Mbps transmission in the 2.4 GHz ISM band using either FHSS or DSSS.

What is 802.11b?

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

How fast is 802.11b?

The IEEE 802.11b standard has a nominal speed of 11 megabits per second (Mbps). However, depending on signal quality and how many other people are using the wireless Ethernet through a particular Access Point, usable speed will be much less (on the order of 4 or 5 Mbps, which is still substantially faster than most dialup, cable and DSL modems).

What is 802.11a?

802.11a the second revision of 802.11 that operates in the unlicensed 5 GHz band and allows transmission rates of up to 54Mbps. 802.11a uses OFDM (orthogonal frequency division multiplexing) as opposed to FHSS or DSSS. Higher data rates are possible by combining channels. Due to higher frequency, range is less than lower frequency systems (i.e., 802.11b and 802.11g) and can increase the cost of the overall solution because a greater number of access points may be required. 802.11a is not directly compatible with 802.11b or 802.11g networks. In other words, a user equipped with an 802.11b or 802.11g radio card will not be able to interface directly to an 802.11a access point. Multi-mode NICs will solve this problem.

What is 802.11g?

802.11g is an extension to 802.11b. 802.11g increases 802.11b's data rates to 54 Mbps and still utilize the 2.4 GHz ISM. Modulation is based upon OFDM (orthogonal frequency division multiplexing) technology. An 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. The range at 54 Mbps is less than for 802.11b operating at 11 Mbps.

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

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

What is Wi-Fi?

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

What types of devices use the 2.4GHz Band?

Various spread spectrum radio communication applications use the 2.4 GHz band. This includes WLAN systems (not necessarily of the type IEEE 802.11b), cordless phones, wireless medical telemetry equipment and Bluetooth™ short-range wireless applications, which include connecting printers to computers and connecting modems or hands-free kits to mobile phones.

Does the 802.11 interfere with Bluetooth devices?

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

Can radio signals pass through walls?

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

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

Factors of interference:
1. Obstacles: walls, ceilings, furniture… etc.
2. Building Materials: metal door, aluminum studs.
3. Electrical devices: microwaves, monitors, electric motors.

Solution :
1.Minimizing the number of walls and ceilings
2.Antenna is positioned for best reception
3.Keep WLAN products away from electrical devices, eg: microwaves, monitors, electric motors,…, etc.
4. Add additional APs if necessary.

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

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

What is Ad Hoc mode?

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

What is Infrastructure mode?

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

How many Access Points are required in a given area?

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

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

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

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

FHSS uses a narrowband carrier which hops through a predefined sequence of several frequencies at a specific rate. This avoids problems with fixed channel narrowband noise and simple jamming. Both transmitter and receiver must have their hopping sequences synchronized to create the effect of a single "logical channel". To an unsynchronised receivers an FHSS transmission appears to be short-duration impulse noise. 802.11 may use FHSS or DSSS.

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

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

Why the 2.4 Ghz Frequency range?

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

What is Server Set ID (SSID)?

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

What is an ESSID?

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

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

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

What is WEP?

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

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

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

What is a WEP key?

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

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

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

Can the SSID be encrypted?

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

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

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

What are Insertion Attacks?

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

What is Wireless Sniffer?

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

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

Open System:
The default authentication service that simply announces the desire to associate with another station or access point. A station can authenticate with any other station or access point using open system authentication if the receiving station designates open system authentication.
Share Key:
The optional authentication that involves a more rigorous exchange of frames, ensuring that the requesting station is authentic. For a station to use shared key authentication, it must implement WEP.

What is 802.1x?

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

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

force-authorized—disables 802.1X and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
force-unauthorized—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
auto—enables 802.1X and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address.

What is AAA?

AAA is the acronym for Authentication, Authorization, and Accounting and refers to the idea of managing subscribers by controlling their access to the network, verifying that they are who they say they are (via login name and password or MAC address) and accounting for their network usage.

What is RADIUS?

RADIUS stands for Remote Authentication Dial-In User Service. RADIUS is a standard that has been implemented into several software packages and networking devices. It allows user information to be sent to a central database running on a RADIUS Server, where it is verified. RADIUS also provides a mechanism for accounting.

Trouble Shooting

Why none of the LEDs turn on when connect the Prestige's power?

Make sure that you have the correct power adaptor connected to the Prestige, it is plugged into an appropriate power source. Check all cable connections. If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

Why cannot access the Prestige from my computer?

- Check the cable connection from your computer to the Prestige. If the Prestige's IP address has changed, then enter the new one as the website address.
- Make sure your computer's IP address is in the same subnet as the Prestige's IP address.
- Ping the Prestige from a computer on the LAN. Make sure your computer's Ethernet adapter is installed and functioning properly. In the computer, click **Start**, (**All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the Prestige's LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The Prestige should reply
- Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later with JavaScript enabled.
- Make sure you enter the password correctly (the field is case sensitive). If you've forgotten the Prestige's password, use the **RESET** button. Press the button in for about 10 seconds (or until the **SYS** LED starts to blink), then release it. It returns the Prestige to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.).

Why cannot access the Internet?

Verify the Internet connection settings in the wizard. Make sure you entered correct user name and password if you are using **PPPoE.**
Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use two ways:

Check if the 'MAC address' is valid

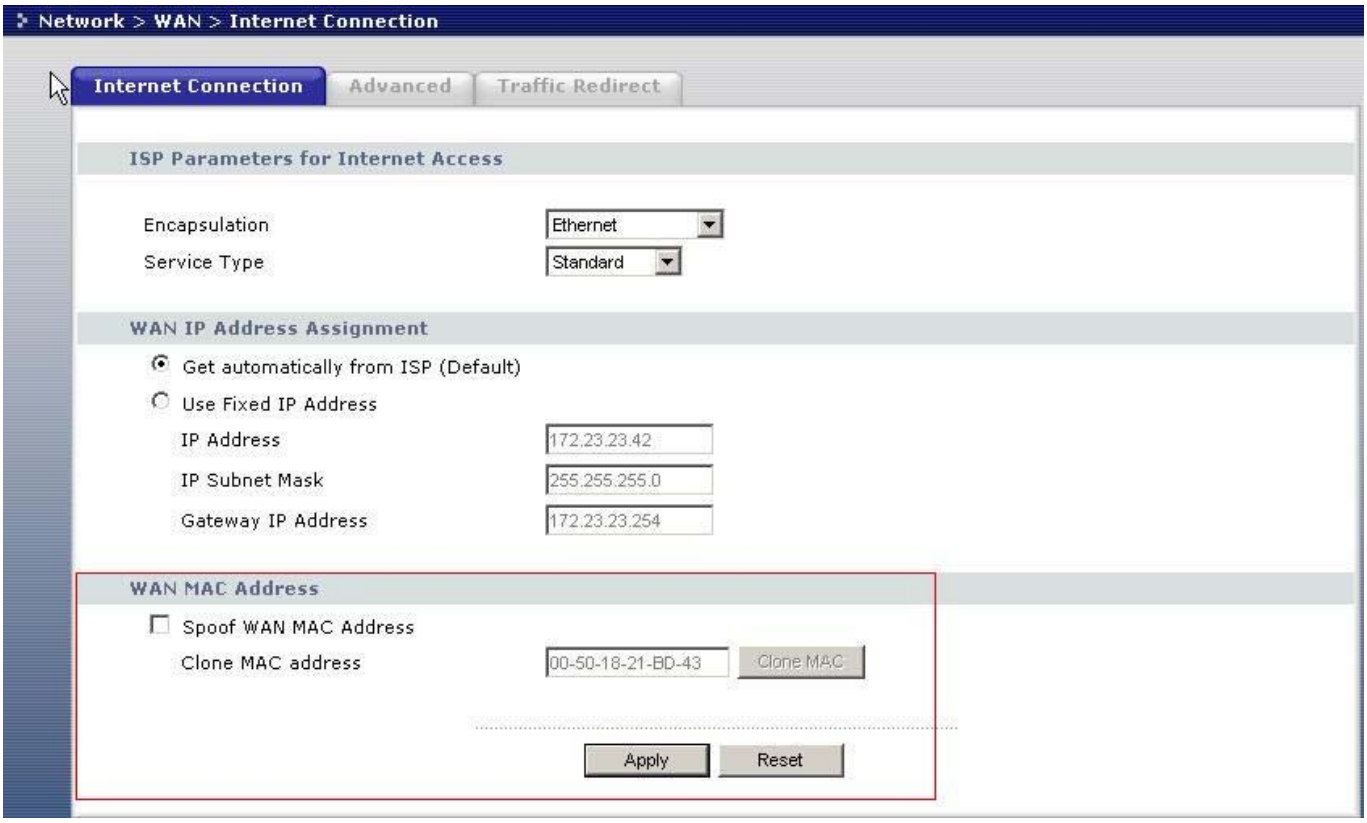
Check if the 'Host Name' is valid, e.g., @home

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

1. Your ISP checks the 'MAC address'

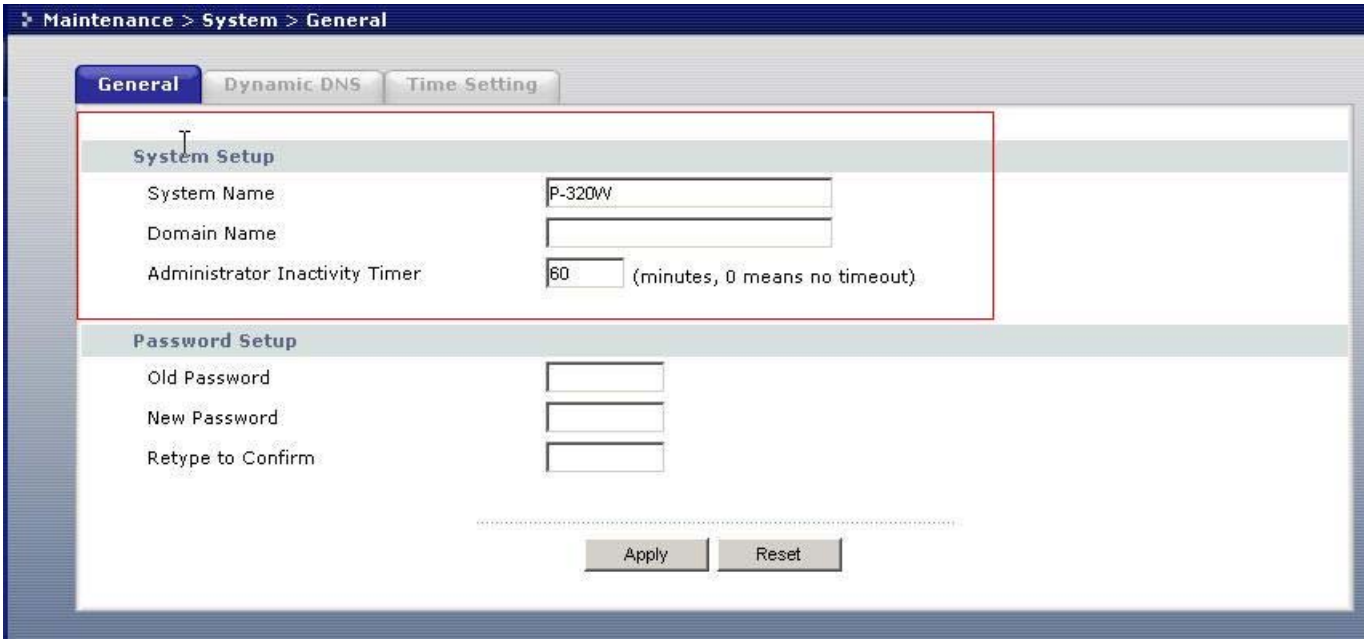
Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for the authentication. So, if a new network card is used or the Prestige is attached to the cable modem directly, the ISP will reject the DHCP discovery from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

The Prestige supports to clone the MAC from the first PC the ISP installed to be its WAN MAC. To clone the MAC from the PC you need to enter that PC's IP in Network > WAN > Internet Connection. Once the MAC is received by the Prestige, the WAN MAC will be updated and used for the ISP's authentication.



2. Your ISP checks the 'Host Name'

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



Unable to run applications

1. Currently, the applications supported in SUA mode are listed in the ZyXEL SUA Support Table. Please check all the required settings suggested in the table to configure your P320W.
2. If your application is not in the table or it is in the table but still does not work, please configure the workstation which runs the applications as the SUA default server and try again.
3. If it still does not work then please provide the application name, version for our analysis.

ZyXEL SUA Supporting Table

Application	Outgoing Connection	Incoming Connection
HTTP	None	80/client IP
FTP	None	21/client IP
TELNET	None	23/client IP (and remove Telnet filter in WAN port)
POP3	None	110/clinet IP
SMTP	None	25/client IP

mIRC	None for Chat. For DCC, please set Default/Client IP	
Windows PPTP	None	1723/client IP
ICQ 99a	None for Chat. For DCC, please set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
ICQ 2000b	None for Chat	None for Chat
ICQ Phone 2000b	None	6701/client IP
Cornell 1.1 Cu-SeeMe	None	7648/client IP
White Pine 3.1.2 Cu-SeeMe	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	None	1720/client IP 1503/client IP
Cisco IP/TV 2.0.0	None	
RealPlayer G2	None	
VDOLive	None	
Quake1.06	None	Default/client IP
QuakeII2.30	None	Default/client IP
QuakeIII1.05 beta	None	
StartCraft	6112/client IP	
Quick Time 4.0	None	
pcAnywhere 8.0	None	5631/client IP 5632/client IP 22/client IP
IPsec (ESP tunneling mode, NAT-T tunnel/transport)	None (one client only)	Default/Client

Microsoft Messenger Service 3.0	6901/client IP	6901/client IP
Microsoft Messenger Service 4.6/ 4.7/ 5.0 (none UPnP)	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
e-Donkey	None	4661 - 4662/client IP
POLYCOM Video Conferencing	None	Default/client IP
iVISTA 4.1	None	80/server IP
Microsoft Xbox Live	None	N/A