

LTE5121

LTE Indoor Wi-Fi VoIP IAD

Support Note

Nov 2012

Edition 1.0

Contents

General Application Note	3
Why use LTE5121?	3
Key Application Scenario	4
Access Application Notes	5
Web GUI	5
LTE5121 WAN setup	7
VoIP configuration	9
NAT Introduction	12
Data Service FTP Downloading Scenario	13
Port Forwarding Configuration	14
File Sharing	15
Media Server Feature	17
QoS Support	17
Wireless Application Notes	23
Wireless Introduction	23
Wireless Configuration	32
WPS Application Notes	38
What is WPS?	38
WPS configuration	39
Maintenance Log	40
Maintenance Tool	41
WAN (LTE) connection Information	43
Product FAQ	46
Wireless FAQ	51

General Application Note

Why use LTE5121?

High performance and capacity

The MIMO products support state-of-the-art Matrix A and Matrix B modes with an aggregated throughput of up to 100 Mbps DL and 50 Mbps UL.

Maximum mobility freedom

The LTE5121 comes with the carrier-standard PCIe LTE module that complies to the 3GPP Release 8 Standard. The device provides users with wireless broadband connectivity for the freedom to surf the Internet and access any information at home, in the office or anywhere under LTE coverage without wire connection.

Ultimate wireless broadband technology

The LTE5121 provides high-speed LTE access services to meet the worldwide market requirements of mobile broadband connectivity; it also features built-in 802.11n WLAN functions that eliminate troublesome wirings jobs in the house. Two telephony service lines are provided using VoIP technology with SIP signaling protocol.

SIP-Based VoIP communications

The LTE5121 supports SIP (RFC3261)-based VoIP signaling suitable for IP telephony service deployments while the sophisticated voice compression and QoS mechanisms provide high-quality voice communications.

Advanced IP networking features

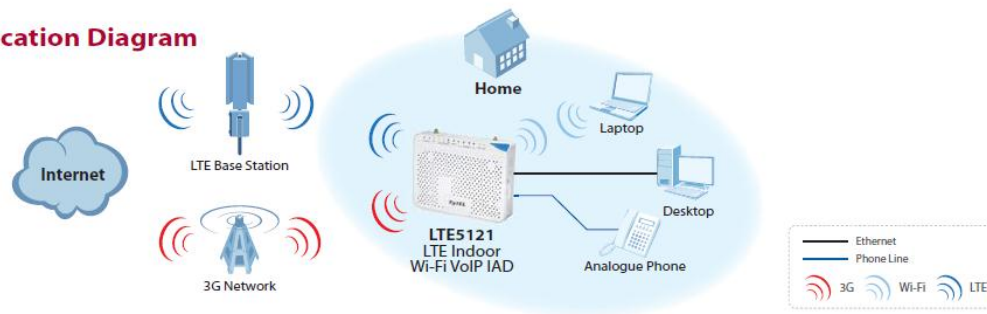
The LTE5121 supports advanced IP networking functionalities, including all Secure NAT Router features needed to access the Internet safely. The LTE5121 also provides remote management capability through TR-069 or OMA-DM.

Software upgrades Over-the-Air (OTA)

Through the LTE radio interface, the CPE supports full configuration capabilities through TR-069 and software upgrades.

Key Application Scenario:

Application Diagram



The ZyXEL device provides shared Internet access by LTE, the most advanced wireless technology. The LTE5121 serves as a home gateway, providing high speed Internet access, and high quality of VoIP service.

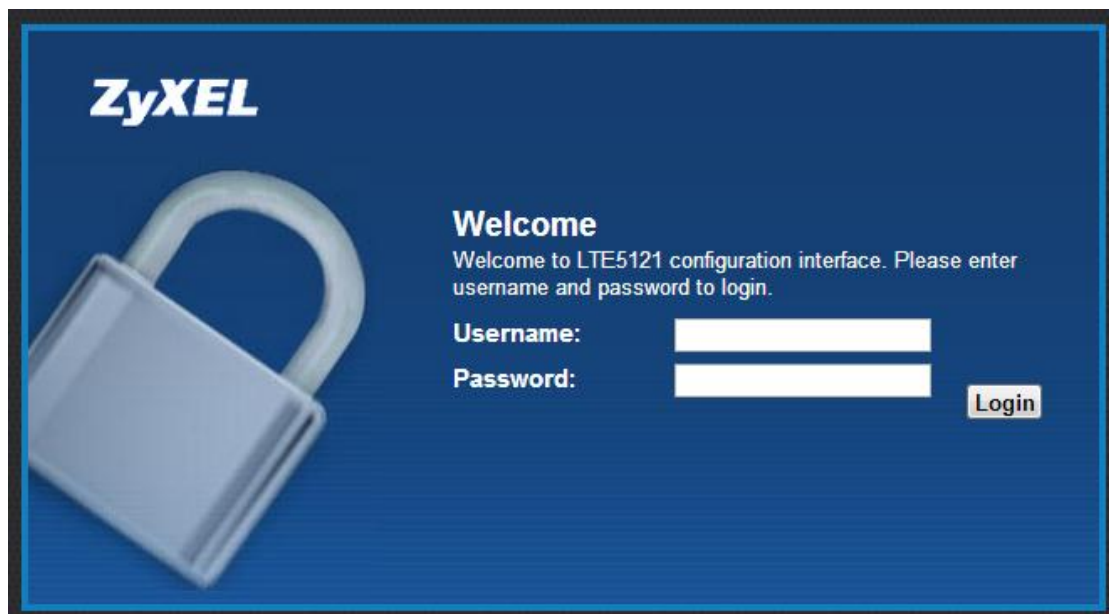
Access Application Notes

Web GUI

The following procedure describes the most typical operation of the device using a browser. The device features an embedded Web server that allows you to use Web browser to configure it. Please make sure there is no Telnet or Console login session before configuring the router using a browser.

- Accessing the Prestige Web

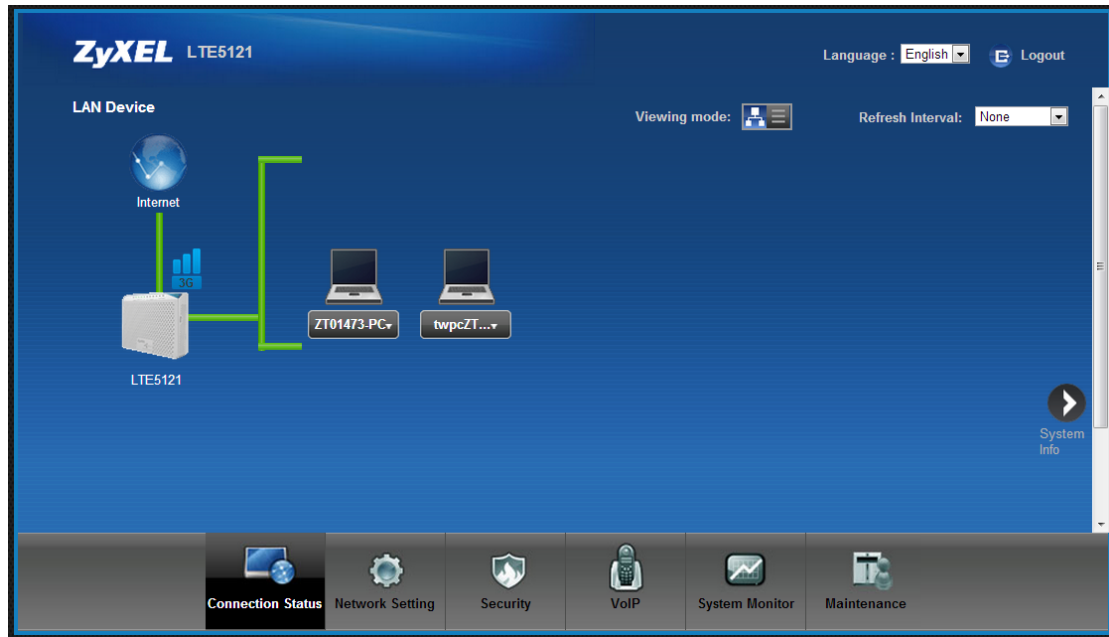
Please enter the LAN IP address of the Prestige router in the URL location to retrieve the login web page from the device. The default LAN IP of the device is 192.168.1.1. See the example below.



- Log into the LTE5121 via Web GUI.

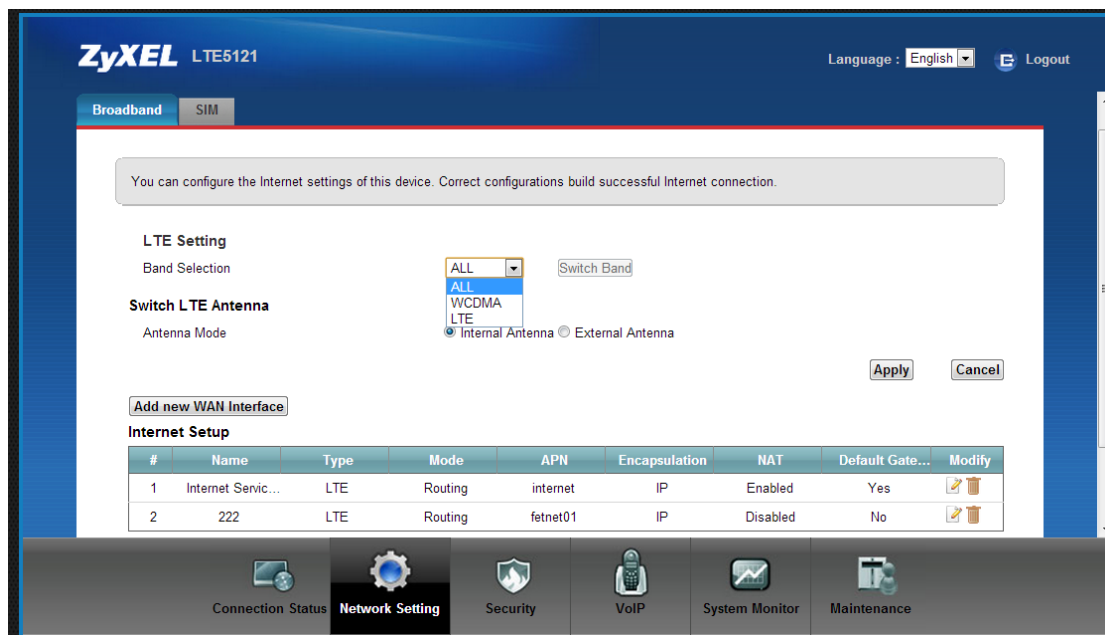
1. Set up your PC/NB IP address to be a DHCP client.
2. Connect to a LAN port of LTE5121 via RJ45 Ethernet cable and open your Web browser.
3. The default IP of LTE5121 is 192.168.1.1

Username/password = admin/1234

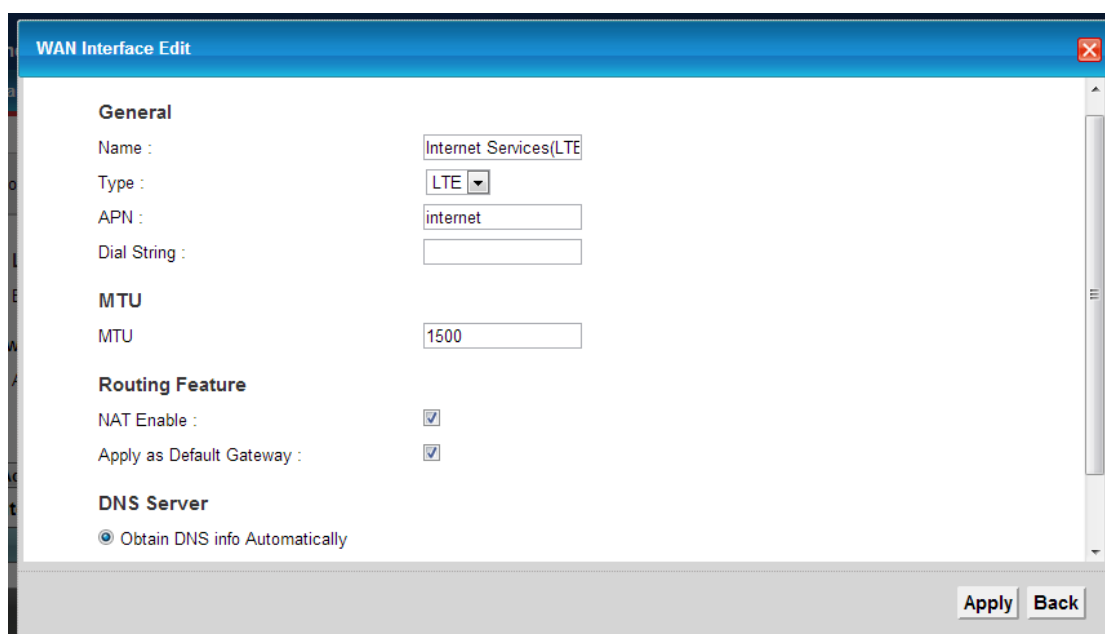


LTE5121 WAN setup:

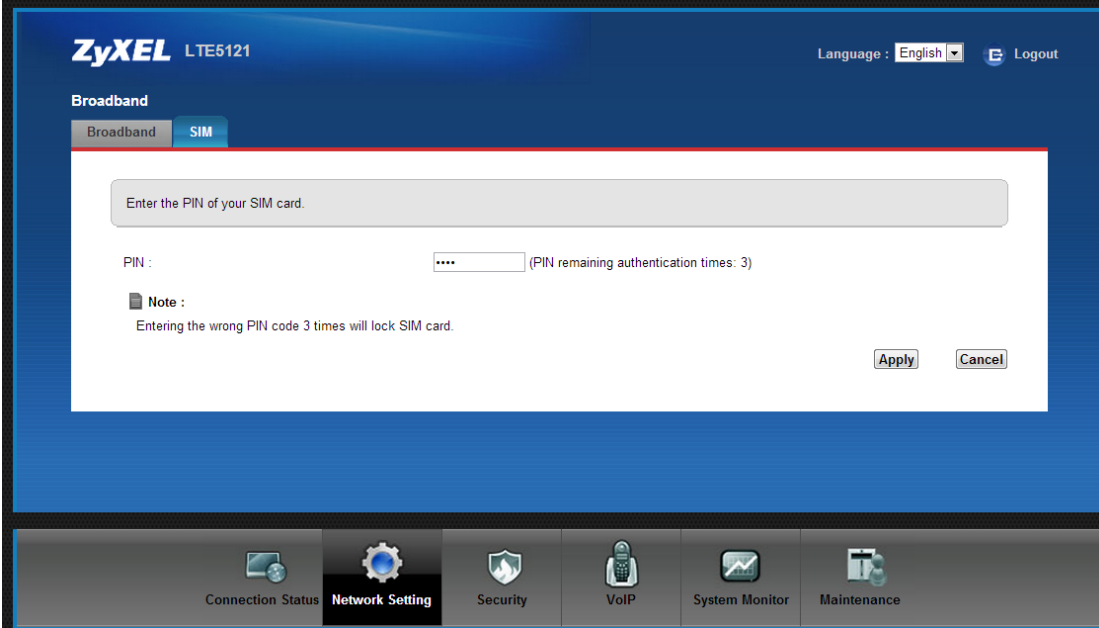
1. Go to **Networking Setting > Broadband** and select the **Broadband** tab.
2. In LTE setting, you can either choose **LTE** or **WCDMA(3G)** or pick **ALL** for auto band selection.



3. Fill in the **APN** field (should be obtained from ISP), this indicates the particular P-GW (particular IP network defined in ISP) for this WAN interface.



4. You should also enter the **SIM card PIN**.



The screenshot shows the ZyXEL LTE5121 web interface. At the top, the logo 'ZyXEL LTE5121' is on the left, and 'Language : English' and 'Logout' are on the right. Below the logo, there are tabs for 'Broadband' and 'SIM'. The 'SIM' tab is selected. The main content area has a header 'Enter the PIN of your SIM card.' followed by a text input field. Below the input field, it says 'PIN : ' followed by a masked input field (four dots) and '(PIN remaining authentication times: 3)'. A 'Note' section states: 'Entering the wrong PIN code 3 times will lock SIM card.' At the bottom right of the form are 'Apply' and 'Cancel' buttons. A navigation bar at the very bottom contains icons for 'Connection Status', 'Network Setting' (which is highlighted), 'Security', 'VoIP', 'System Monitor', and 'Maintenance'.

ZyXEL LTE5121

Language : English Logout

Broadband SIM

Enter the PIN of your SIM card.

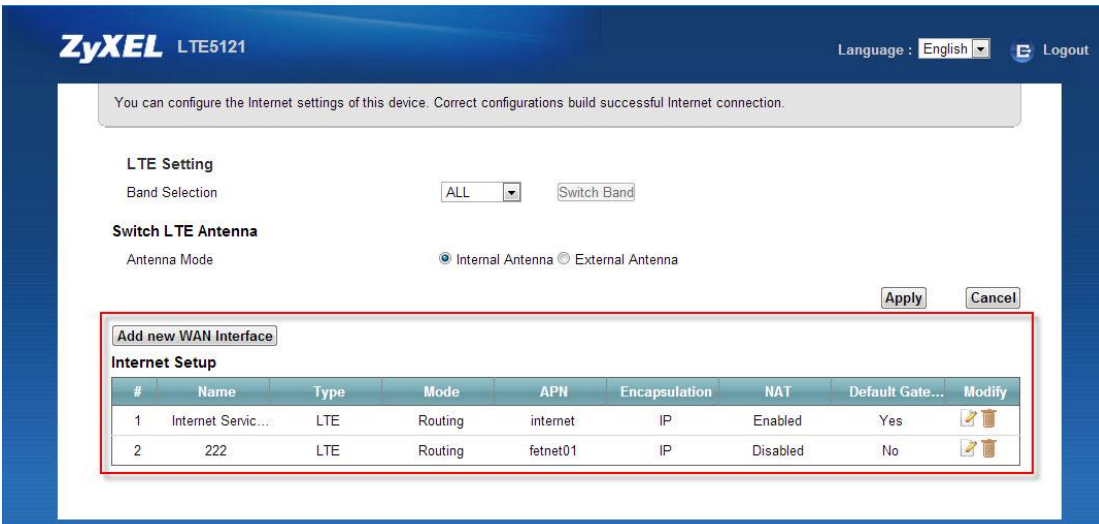
PIN : (PIN remaining authentication times: 3)

Note :
Entering the wrong PIN code 3 times will lock SIM card.

Apply Cancel

Connection Status Network Setting Security VoIP System Monitor Maintenance

5. You can also add multiple WAN interfaces by clicking **“Add New WAN Interface”**.



The screenshot shows the ZyXEL LTE5121 web interface for 'Internet Setup'. At the top, the logo 'ZyXEL LTE5121' is on the left, and 'Language : English' and 'Logout' are on the right. Below the logo, there is a message: 'You can configure the Internet settings of this device. Correct configurations build successful Internet connection.' The 'LTE Setting' section includes 'Band Selection' with a dropdown menu set to 'ALL' and a 'Switch Band' button. The 'Switch LTE Antenna' section includes 'Antenna Mode' with radio buttons for 'Internal Antenna' (selected) and 'External Antenna'. At the bottom right of this section are 'Apply' and 'Cancel' buttons. Below this is a red-bordered box containing an 'Add new WAN Interface' button and a table titled 'Internet Setup'.

ZyXEL LTE5121

Language : English Logout

You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

LTE Setting

Band Selection ALL Switch Band





Switch LTE Antenna

Antenna Mode Internal Antenna External Antenna

Apply Cancel

Add new WAN Interface

Internet Setup

#	Name	Type	Mode	APN	Encapsulation	NAT	Default Gate...	Modify
1	Internet Servic...	LTE	Routing	internet	IP	Enabled	Yes	 
2	222	LTE	Routing	fetnet01	IP	Disabled	No	 

VoIP configuration

Setting up an SIP Account

The VoIP technology sends voice signals over the Internet Protocol. This allows users to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network.

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks. The Prestige can hold up to two SIP account simultaneously. Please follow the instructions below to configure the SIP accounts properly.

Note: You should have a voice account already set up and have VoIP information from your VoIP service provider prior to configuring a SIP account on the unit. With the account information supplied by your ITSP provider at hand you may start the setup procedure.

1. Go to **VoIP >SIP**, select **“Add New”** for the Service selection and enter the SIP server IP address supplied by your SIP service provider.

The screenshot displays the ZyXEL LTE5121 web interface. At the top, the header includes the ZyXEL logo, the model number LTE5121, a language dropdown set to English, and a Logout button. Below the header, there are two tabs: 'SIP Service Provider' (active) and 'SIP Account'. A grey informational box states: 'SIP Service Provider offers services of making Internet calls using VoIP technology. You may need to consult your SIP Service Provider for the following settings. This configuration should be used in conjunction with SIP Account.'

SIP Service Provider Selection

Service Provider Selection :

General

SIP Service Provider : ☒ Enable SIP Service Provider

SIP Service Provider Name :

SIP Local Port : (1025-65535)

Main SIP Server Address :

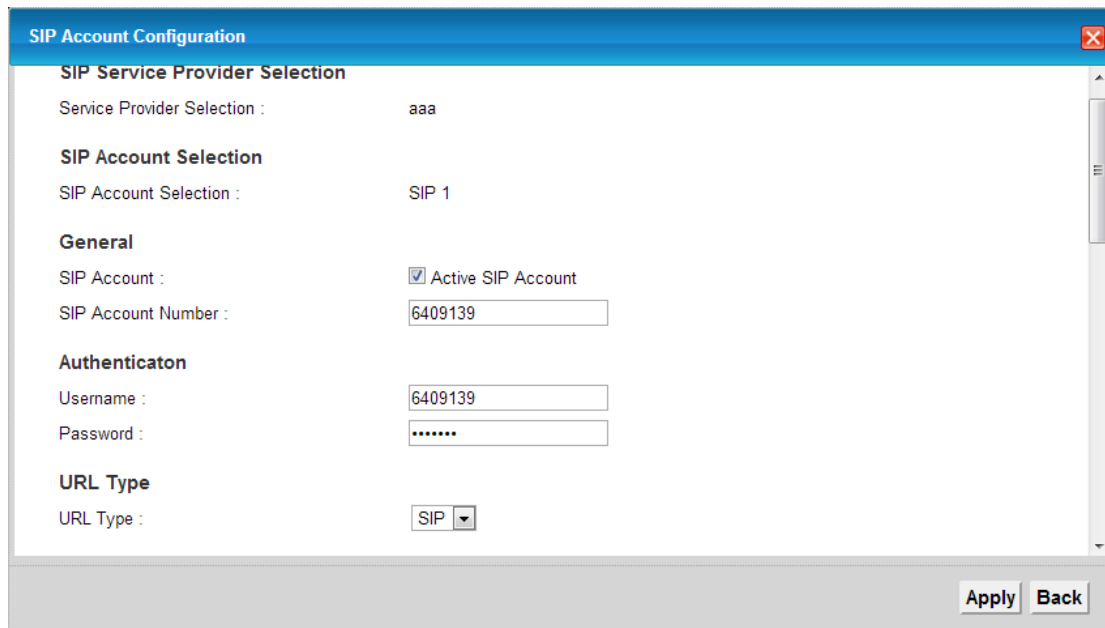
SIP Server Port : (1025-65535)

REGISTER Server Address :

REGISTER Server Port : (1025-65535)

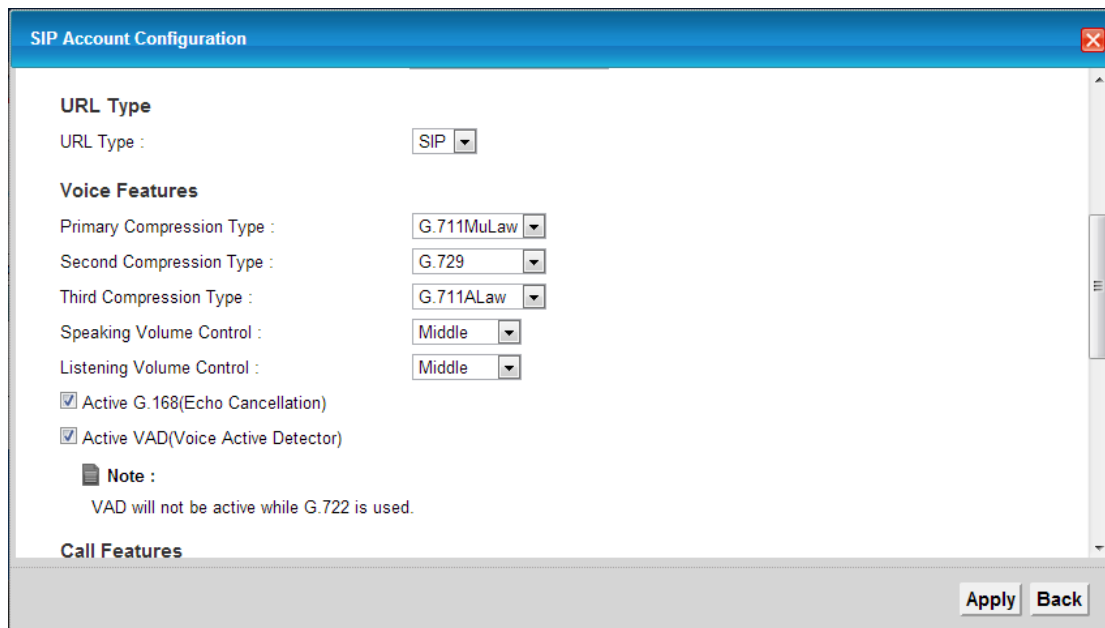
At the bottom of the interface is a navigation bar with icons and labels for: Connection Status, Network Setting, Security, VoIP (highlighted), System Monitor, and Maintenance.

2. Click on the **"SIP Account"** tab to configure the SIP account.
3. Click Edit icon for **"SIP1"** and configure the SIP account.



The image shows the 'SIP Account Configuration' window. It has a blue title bar with the text 'SIP Account Configuration' and a close button. The window is divided into several sections: 'SIP Service Provider Selection' with 'Service Provider Selection : aaa', 'SIP Account Selection' with 'SIP Account Selection : SIP 1', 'General' with 'SIP Account : ☒ Active SIP Account' and 'SIP Account Number : 6409139', 'Authentication' with 'Username : 6409139' and 'Password :', and 'URL Type' with 'URL Type : SIP'. At the bottom right, there are 'Apply' and 'Back' buttons.

4. Fill in the SIP number and the account username and password. Leave the Advanced setting unchanged.



The image shows the 'SIP Account Configuration' window, now showing the 'Voice Features' and 'Call Features' sections. The 'URL Type' section is still visible at the top. The 'Voice Features' section includes: 'Primary Compression Type : G.711MuLaw', 'Second Compression Type : G.729', 'Third Compression Type : G.711ALaw', 'Speaking Volume Control : Middle', 'Listening Volume Control : Middle', and two checked checkboxes: 'Active G.168(Echo Cancellation)' and 'Active VAD(Voice Active Detector)'. Below these is a 'Note' section with a document icon and the text 'VAD will not be active while G.722 is used.' The 'Call Features' section is partially visible at the bottom. At the bottom right, there are 'Apply' and 'Back' buttons.

After the SIP account is properly configured, the LTE5121 will automatically register the configured SIP account with assigned SIP server. If it does not, you can go to the Status page, scroll down to the SIP account status section, and click “**Register**” to register the SIP account manually.

Or you can also click “**Unregister**” to unregister the SIP account manually.

The screenshot displays the ZyXEL LTE5121 web management interface. At the top, the header shows 'ZyXEL LTE5121' and a language dropdown set to 'English' with a 'Logout' button. The main content area is divided into several sections:

- SSID Information:** A list of three SSIDs with their respective status and security modes.

SSID	Status	Security Mode
ZyXEL_BE19	Off	WPA2-PSK mixed
ZyXEL_BE1A	Off	WPA2-PSK mixed
ZyXEL_BE1B	Off	WPA2-PSK mixed
- System Status:** A summary of system health and resource usage.

System Status	
System Up Time:	5:34
Current Date/Time:	Mon Nov 26 12:17:50 CET 2012
System Resource:	
- CPU Usage:	1.0%
- Memory Usage:	55.8%
- Registration Status:** A table showing the status of two SIP accounts.

Account	Action	Account Status	URI
SIP 1	Register	In-Active	6409139@59.124.163.156
SIP 2	Unregister	Registered	6003@59.124.163.156

At the bottom, a navigation bar contains icons and labels for 'Connection Status', 'Network Setting', 'Security', 'VoIP', 'System Monitor', and 'Maintenance'.

NAT Introduction

- What is NAT?

NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated as the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on the incoming packets back into local IP addresses. The IP addresses for NAT can be either fixed or dynamically assigned by the ISP.

In addition, you can designate servers, e.g., a Web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, the NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the CPE, thus preventing intruders from probing your network.

For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

- How does NAT work?

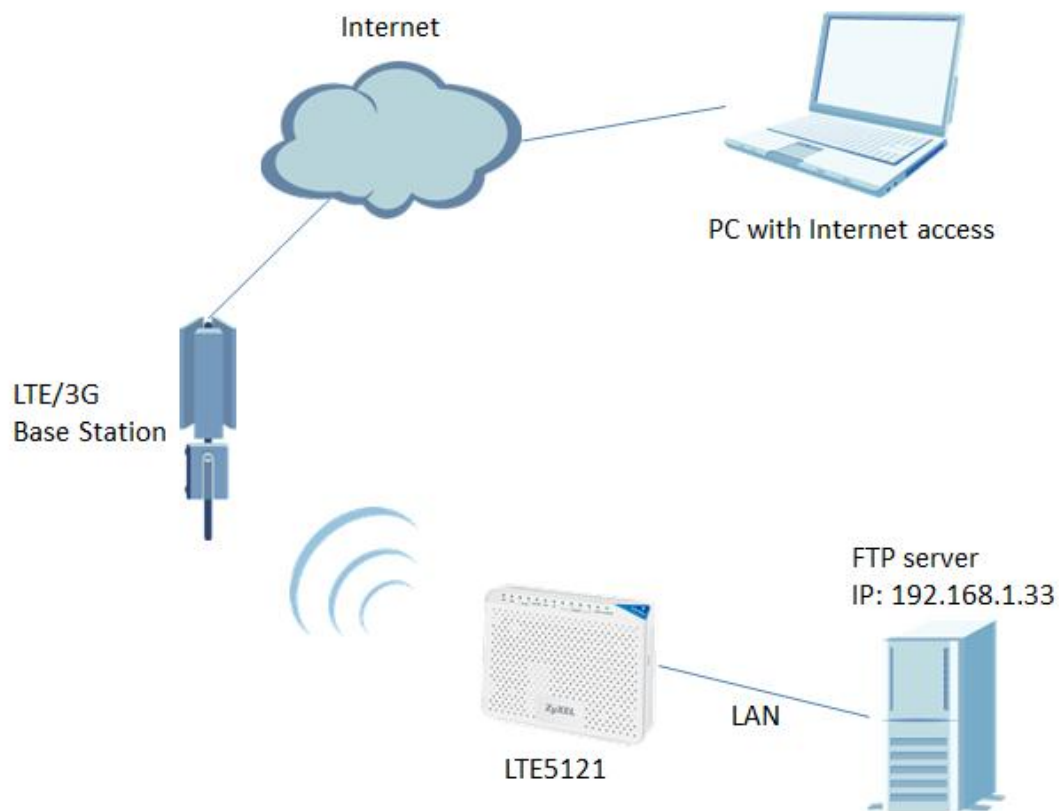
We define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Addresses (IGA). The term 'inside' refers to the set of networks that are subject to translation.

The NAT operates by mapping the ILA to the IGA required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers) and then forwards each packet to the Internet ISP, thus making them appear as if they came from the NAT system itself (e.g., the CPE router).

The CPE keeps track of the original addresses and port numbers, so the incoming reply packets can have their original values restored.

Data Service FTP Downloading Scenario

- Topology



NAT provides system administrators with an easy solution to create a private IP network for security and IP management. Powered by NAT technology, the LTE5121 supports complete NAT mapping and most popular Internet multimedia applications. This feature is best demonstrated with the NAT port forwarding feature implemented in the CPE. In a scenario shown in the above diagram, we have an FTP server installed behind the CPE with an IP assigned by the local DHCP server (192.168.1.33). How should we configure the LTE5121, so that the notebook at the WAN site can access the FTP server? The following step-by-step guide illustrates the setup.

PS: Make sure that NAT is enabled on the WAN interface.

Port Forwarding Configuration

a. Create a port forwarding rule for the FTP server.

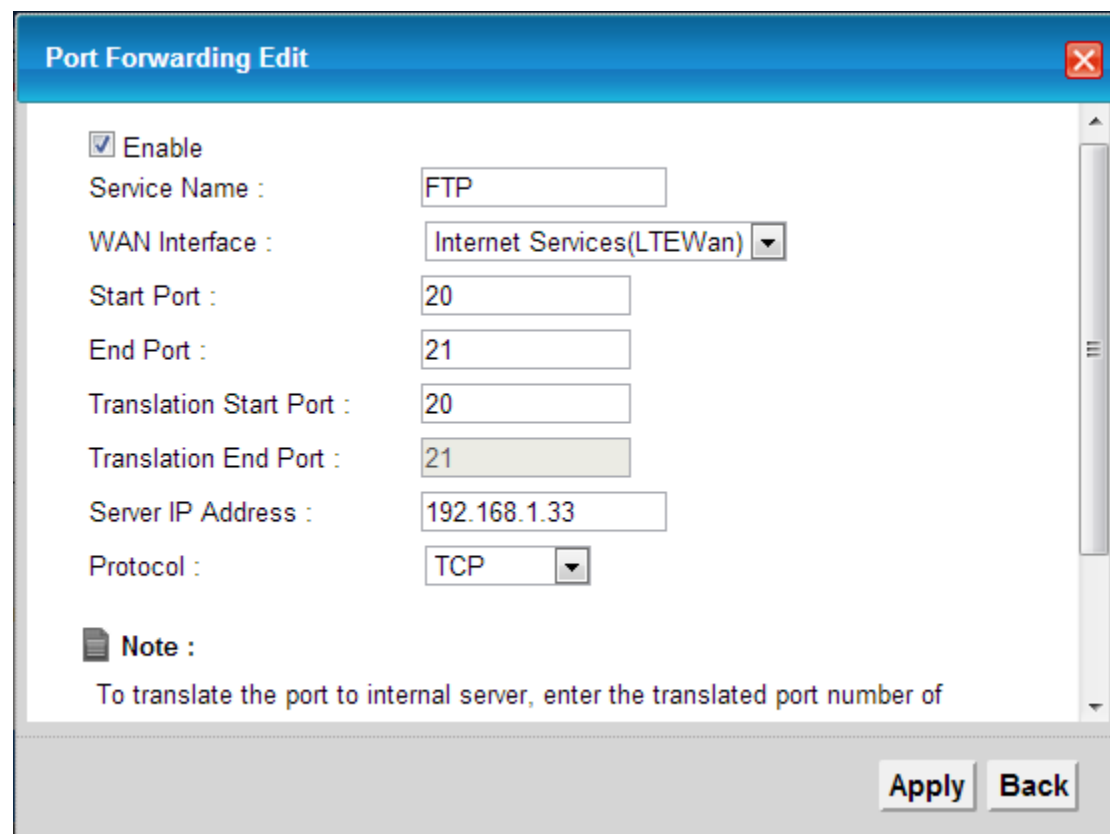
1. Go to **Network Setting > NAT > Port Forwarding** and click “**add new rule**”.

2. Select the Service Name, e.g. “FTP”.

3. Select the WAN Interface, e.g. “EtherWAN1”.

4. Enter the Server IP Address, e.g. “192.168.1.33”.

5. Click **Apply**.



The screenshot shows a window titled "Port Forwarding Edit" with a blue header bar and a red close button. The window contains the following configuration fields:

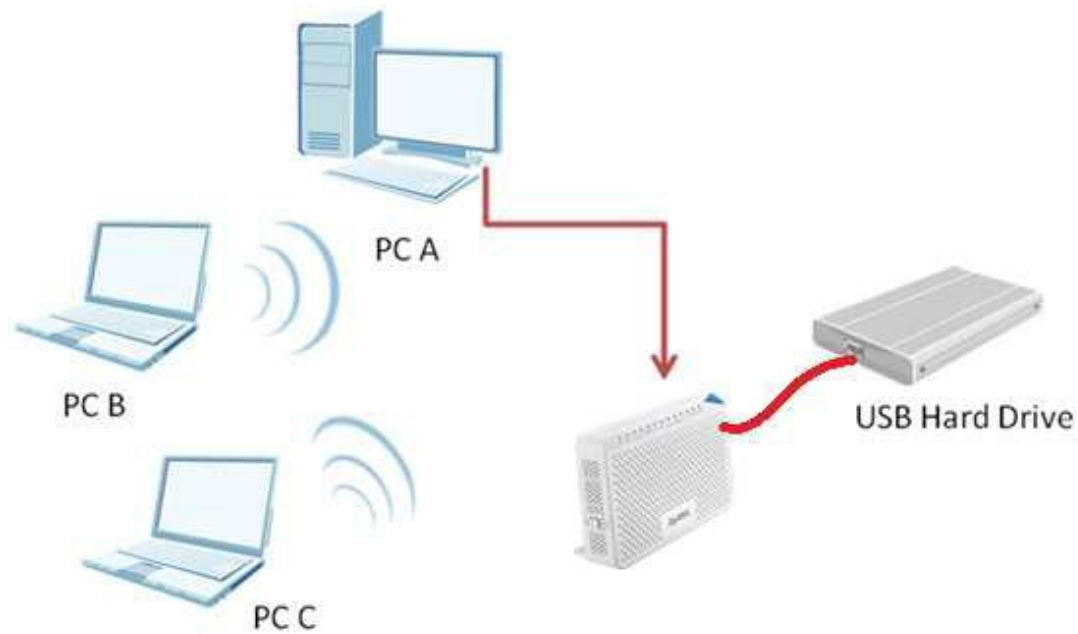
- ☒ Enable
- Service Name :
- WAN Interface : (dropdown menu)
- Start Port :
- End Port :
- Translation Start Port :
- Translation End Port :
- Server IP Address :
- Protocol : (dropdown menu)

Below the fields is a "Note" section with a document icon and the text: "To translate the port to internal server, enter the translated port number of".

At the bottom right of the window are two buttons: "Apply" and "Back".

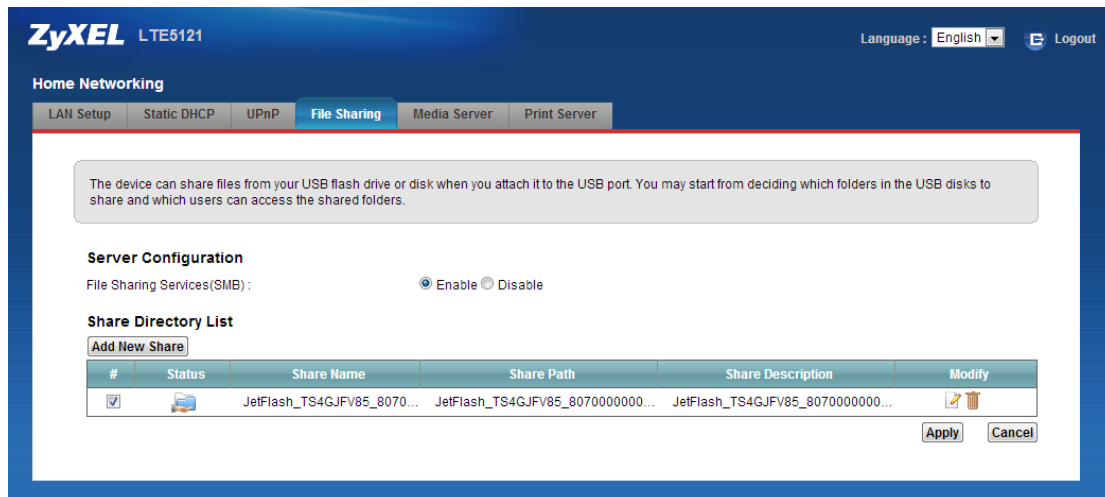
File Sharing

This feature allows sharing files on a USB memory stick or hard drive connected to the LTE5121 with other users on the network. The topology shown below allows PCs A, B and C to access files on the USB Hard drive.

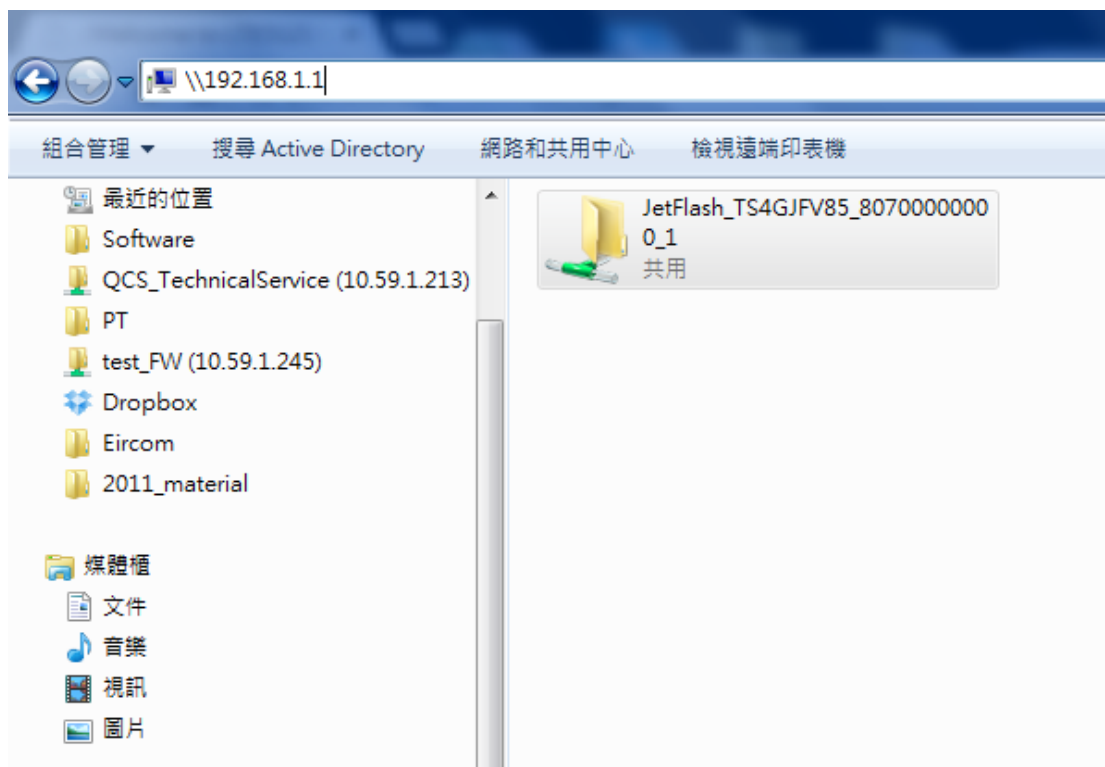


1. Plug a Flash disk into the USB port.
2. Go to **Network Setting > Home Networking**.
3. Select the “**Enable**” button of File Sharing Service (SMB) function.
4. Set the Workgroup name (e.g. Workgroup).
5. Select the Folder for sharing.
6. Click on “**Apply**”.

When the File Sharing feature is enabled, LTE5121 will find the attached USB hard drive.

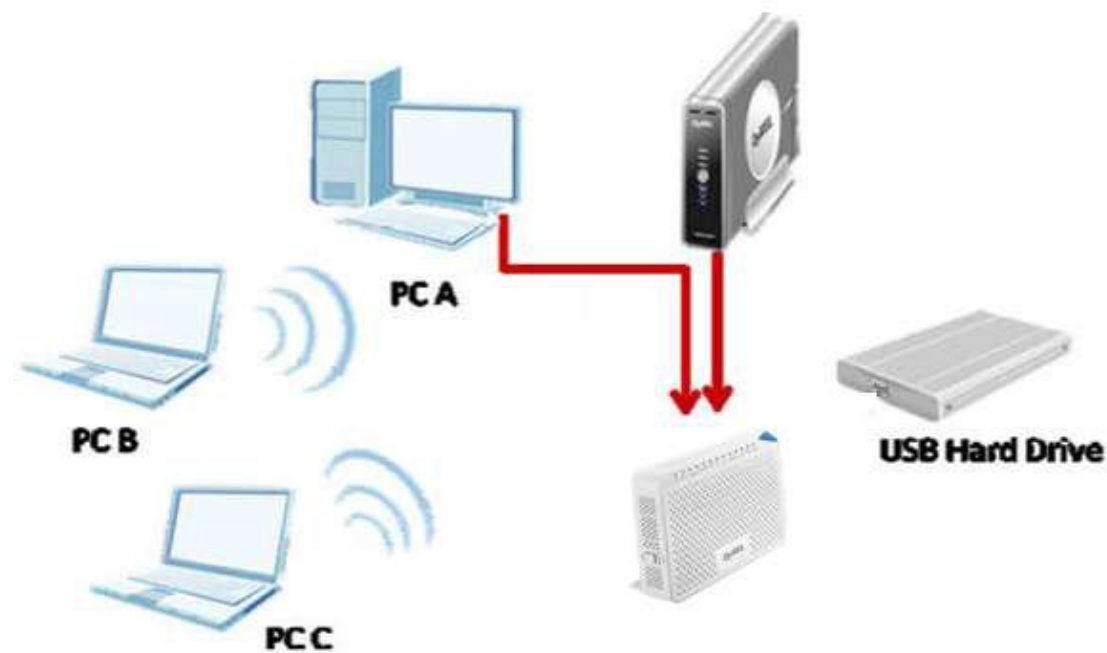


7. Go to “Windows Explorer” and enter [\\192.168.1.1](http://192.168.1.1), you will find the hard drive which is connected to the router.

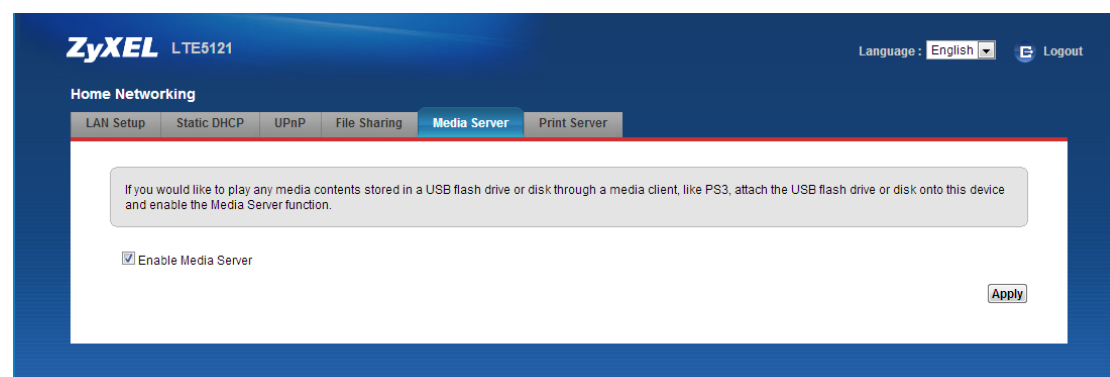


Media Server Feature

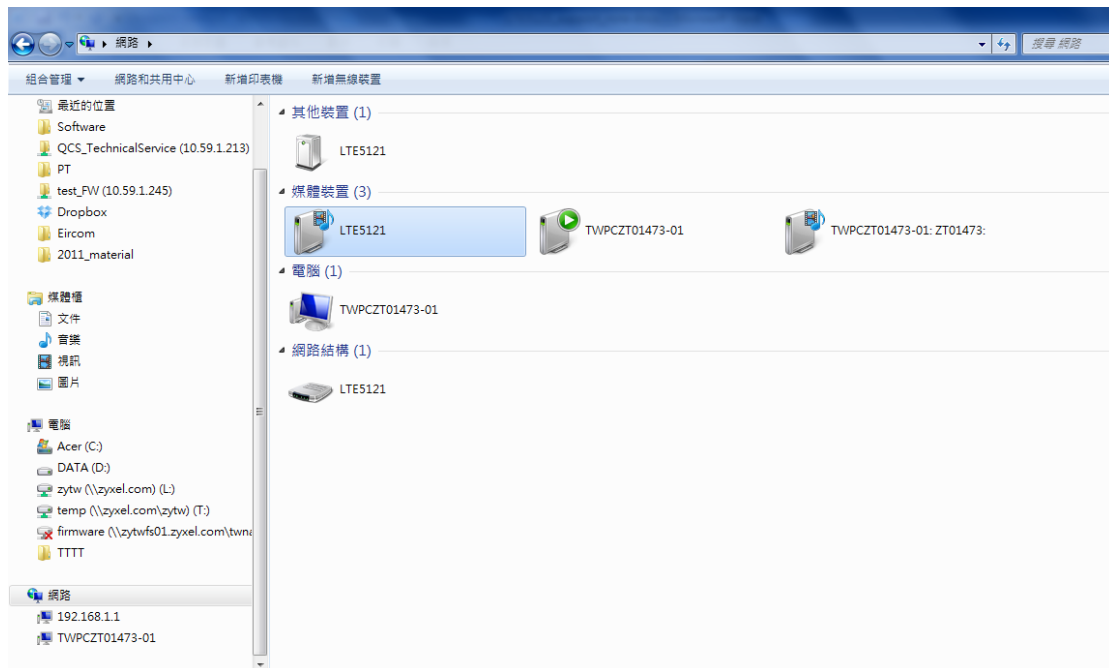
Using the media server feature to play media files on a the PC, this section shows you how the media server feature works with the Windows Media Player in Windows 7 (if the user does not have a media player as suggested in the User Guide) to play music or video from a USB disk and NSA-210 which is connected to the LAN port.



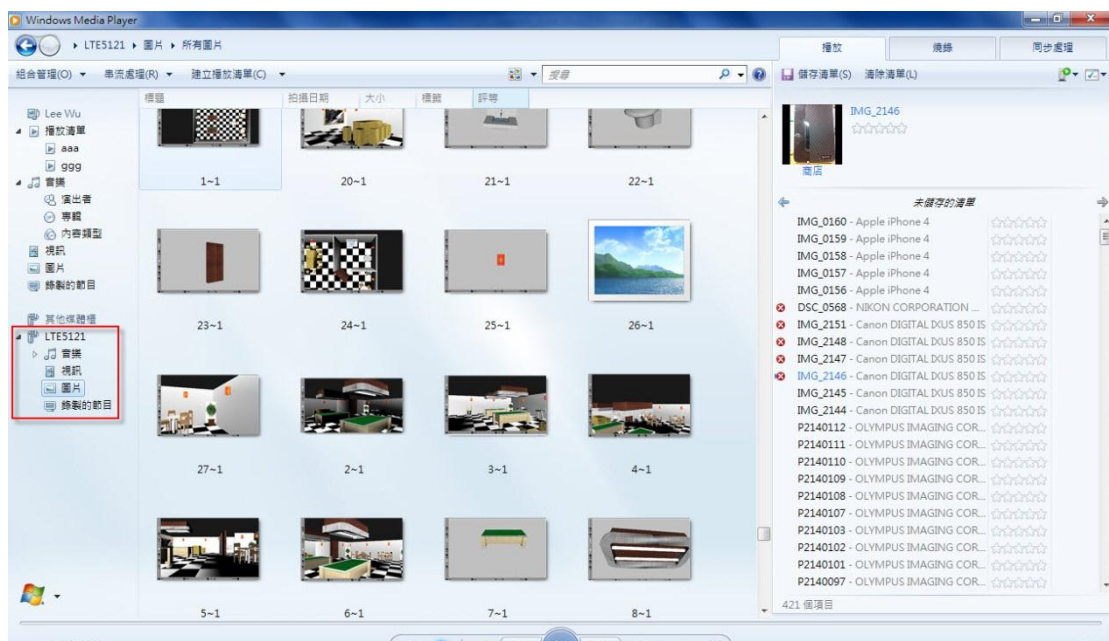
1. Go to **Network Setting > Home Networking > Media Server**.
2. Click on **“Enable Media Server”**.



3. Double click on the media device.



4. Windows Media Player will be opened, and you can browse various types of media files from the USB hard drive which is attached to the LTE5121.



QoS Support

Introduction to QoS

- Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and to the networking methods used to control the use of bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.
- Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network unfit for time critical applications such as video-on-demand and VoIP.

1. Click **Network Setting > QoS > General** and activate the QoS service, then set the Maximum Upstream bandwidth value to 512 to fully utilize WAN bandwidth.

The screenshot shows the ZyXEL LTE5121 web interface. At the top, the logo 'ZyXEL LTE5121' is on the left, and 'Language : English' and 'Logout' are on the right. Below the header, the 'QoS' section is active, with tabs for 'General', 'Queue Setup', 'Class Setup', and 'Monitor'. The 'General' tab is selected, showing a description: 'Quality of Service (QoS) defines the traffic priority of Internet services to the home network.' Below this, there is a checkbox for 'Active QoS' which is checked. Next to it is a text field for 'WAN Managed Upstream Bandwidth' with the value '512' and '(kbps)' next to it. Below that is a dropdown menu for 'Traffic priority will be automatically assigned by' with 'None' selected. A 'Note' section follows, stating: 'You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically. If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.' At the bottom right of the form are 'Apply' and 'Cancel' buttons. The bottom navigation bar contains icons and labels for 'Connection Status', 'Network Setting' (which is highlighted), 'Security', 'VoIP', 'System Monitor', and 'Maintenance'.

2. Click on **"Queue Setup"**.
3. You can **"Add new Queue"** or **"Edit"** the Queues displayed in the screenshot.
The Priority and Weight can be adjusted

ZyXEL LTE5121 Language : English Logout

QoS

General **Queue Setup** Class Setup Monitor

Queue Setup decides the priority on WAN interfaces. Use this page to configure QoS queue assignment.

Add new Queue

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit(kbps)	Modify
1	⚡	WAN_Default_Queue	WAN	4	1	DT		
2	⚡	LAN_Default_Queue	LAN	4	1	DT		
3	⚡	Fast	WAN	7	3	DT		
4	⚡	Active user	WAN	5	3	DT		
5	⚡	Passive user	WAN	3	3	DT		
6	⚡	Slow	WAN	1	3	DT		

Connection Status **Network Setting** Security VoIP System Monitor Maintenance

4. You can add new Queues for VoIP. Click **"Add new Queue"**, active the new queue, named **"VoIP"**, set priority to 7 and weight to 15.

Add new Queue

☒ Active

Name : VoIP

Interface : WAN

Priority : 7(High)

Weight : 15

Rate Limit : (kbps)

Apply Back

6. Click on the “**Class Setup**” tab to set up QoS Classifiers
7. Configure the first Class rule for VoIP. Select “**VoIP**” in “To Queue:” and input a name for it. E.g. “VoIP_test” as follows:

The screenshot shows the 'Edit Classifier Setting' window. Under 'Class Configuration', 'Active' is checked, 'Class Name' is 'VoIP_test', 'Classification Order' is 'Last', 'Forward To Interface' is 'Unchange', 'DSCP Mark' is 'Unchange', and 'To Queue' is 'VoIP'. Under 'Criteria Configuration', the 'Basic' section has 'From Interface' set to 'Internet Services' and 'Ether Type' set to 'IP (0x0800)'. The 'Source' section is partially visible. 'Apply' and 'Back' buttons are at the bottom right.



8. Enable the **From Interface** and set to “Local”, also enable **Ether Type** criteria and set them accordingly.
9. Set the **Destination IP address** to the SIP server’s IP address.

The screenshot shows the 'Edit Classifier Setting' window with the 'Criteria Configuration' section expanded. In the 'Basic' section, 'From Interface' is set to 'Local' and 'Ether Type' is 'IP (0x0800)'. In the 'Source' section, 'MAC Address', 'IP Address', 'IPv6 Address', and 'Port Range' are all unchecked. In the 'Destination' section, 'MAC Address' is unchecked, 'IP Address' is checked and set to '59.124.163.156', and 'IP Subnet Mask' is set to '255.255.255.255'. 'Exclude' checkboxes are present for each criterion. 'Apply' and 'Back' buttons are at the bottom right.


10. Click “**Apply**”. Now we have completed the Class rule for VoIP service.
11. To make sure the Class rules are correctly configured, you can go to **Network Setting > QoS > Monitor**.
12. Select **5 sec** as the refresh interval time and monitor the ZyXEL device’s QoS

packet statistics.

ZyXEL LTE5121

Language : English   Logout

Monitor shows the statistics of QoS on WAN/LAN interface and the status of Queue Setup.

Monitor
Refresh Interval : 5 seconds 

Status :
Interface Monitor

#	Name	Pass Rate(bps)
1	usb0	8
2	br0	96

Queue Monitor

#	Name	Interface	Pass Rate(bps)	Drop Rate(bps)
1	WAN_Default_Queue	WAN	0	0
2	LAN_Default_Queue	LAN	96	0
3	Fast	WAN	0	0
4	Active user	WAN	0	0
5	Passive user	WAN	0	0
6	Slow	WAN	0	0
7	VoIP	WAN	0	0

Wireless Application Notes

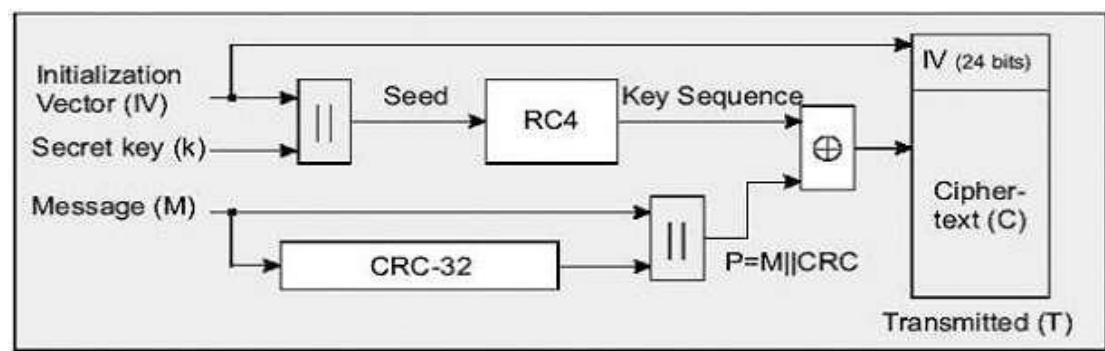
Wireless Introduction

WEP Configuration (Wired Equivalent Privacy) Introduction

The 802.11 standard describes the communication that occurs in wireless LANs. The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping, because the 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.

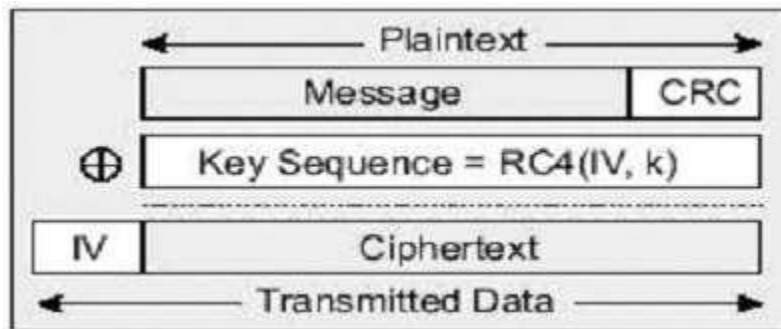
The WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packages are not modified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

The 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.



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. The WEP keys (secret keys) are available in two types, 64-bit and 128-bit. Many times you will see them referenced as 40-bit and 104-bit 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.



Setting up the Access Point

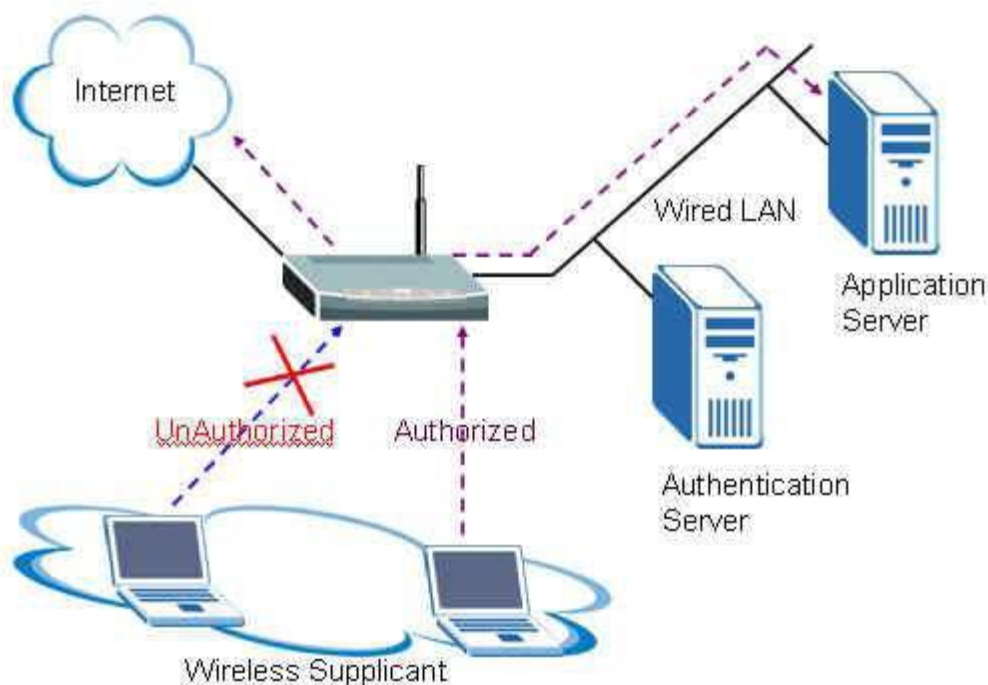


Most access points and clients have the ability to hold up to 4 WEP keys simultaneously. You need to specify one of the 4 keys as the default Key for data encryption. To set up the Access Point, you will need to set one of the following parameters:

- 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.

IEEE 802.1X Introduction

The IEEE 802.1X port-based authentication is designed to prevent unauthorized devices (clients) from gaining access to the network. As the WLANs extend to hotels, airports and corporate lobbies, insecure environments could be created. The 802.1X port-based network access control makes use of the physical access characteristics of **IEEE 802 LAN infrastructures**, such as the 802.3 Ethernet, 802.11 Wireless LAN and ADSL 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. The mechanism is designed to prevent access to that port in case of failure of the authentication process.



The IEEE 802.1X authentication is a client-server architecture delivered through EAPOL (Extensible Authentication Protocol over LAN). The authentication server authenticates each client connected to an Access Point (for Wireless LAN) or switch port (for Ethernet) before allowing access to any services offered by the network. The 802.1X contains three major components:

1. Authenticator:

The device (i.e. Wireless AP) that facilitates authentication for a supplicant (Wireless client) attached to the Wireless network. The 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 authentication server (i.e. RADIUS server), requesting the 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 to the Wireless network. The supplicant requests access to the LAN services and responds to the requests from the authenticator. The station must be running the 802.1X-compliant client software, such as that offered in the Microsoft Windows XP operating system, Meeting House AEGIS 802.1X client and Odyssey 802.1X client.

3. Authentication Server:

The device (i.e. RADIUS server) provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator. The authentication server performs the actual authentication of the client. It validates the identity of the supplicant. Because the authenticator acts as the proxy, the authentication service is transparent to the supplicant. Some Wireless APs (i.e. ZyXEL Wireless AP) have a built-in authentication server, therefore the external RADIUS authentication server is not needed. In this case, the Wireless AP acts as both the authenticator and authentication server.

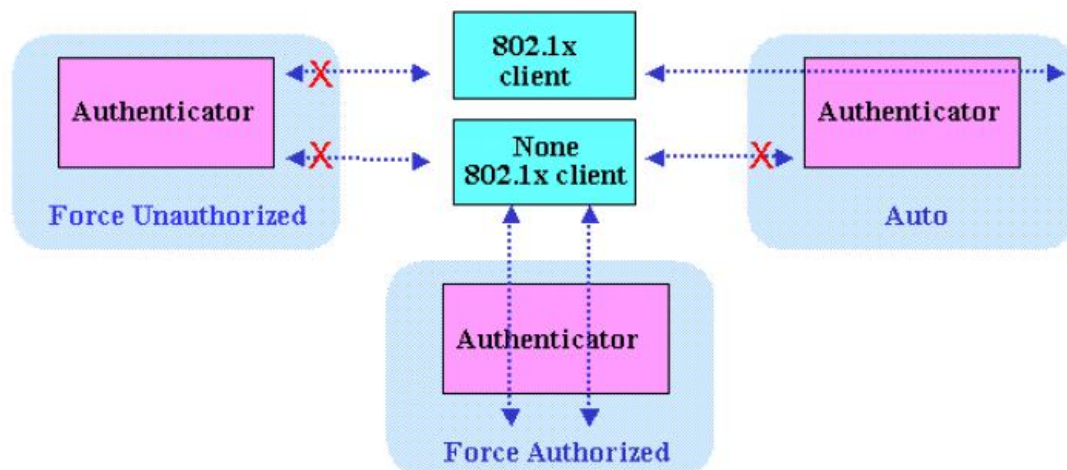
• Authentication Port State and Authentication Control

The port state determines whether or not the supplicant (Wireless Client) is granted access to the network behind the 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 the incoming and outgoing data traffic, except for 802.1x packets. When a supplicant is successfully authenticated, the port transits to the authorized state, allowing all the traffic for 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 three authentication control parameters that are applied in the Wireless AP.



1. Force Authorized: Disables 802.1x authentication and causes the port to transit to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without the 802.1x-based authentication of the client.

This is the default port control setting. While the AP is set up as **Force Authorized**, the 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 the AP is set up as **Force Unauthorized**, Wireless clients (supported 802.1X client or non-802.1X client) can never have the access to the network.

3. Auto: Enables 802.1X authentication and causes the port to begin in the unauthorized state, allowing only the 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 requesting the identity of the client. The authenticator then begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the authenticator using

the client's MAC address. While the AP is setup as **Auto**, only Wireless clients that support the 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 the re-authentication is time out, the authenticator will send the EAP-Request/Identity message to reinitiate the authentication process. In the ZyXEL Wireless AP 802.1X implementation, if you do not specify a time period between re-authentication attempts, the default re-authentication period will be 1,800 seconds (30 minutes).

- **EAPOL (Extensible Authentication Protocol over LAN)**

The authenticators and supplicants communicate with one another by using the Extensible Authentication Protocol (EAP and RFC-2284). The EAP was originally designed to run over PPP and to authenticate dial-in users, but the 802.1X defines an encapsulation method for passing the EAP packets over Ethernet frames.

This method is referred to as the **EAP over LANs, or EAPOL**. Ethernet type of EAPOL is **88-8E**, two octets in length. The EAPOL encapsulations are described for IEEE 802 compliant environment, such as the 802.3 Ethernet, 802.11 Wireless LAN and Token Ring/FDDI.

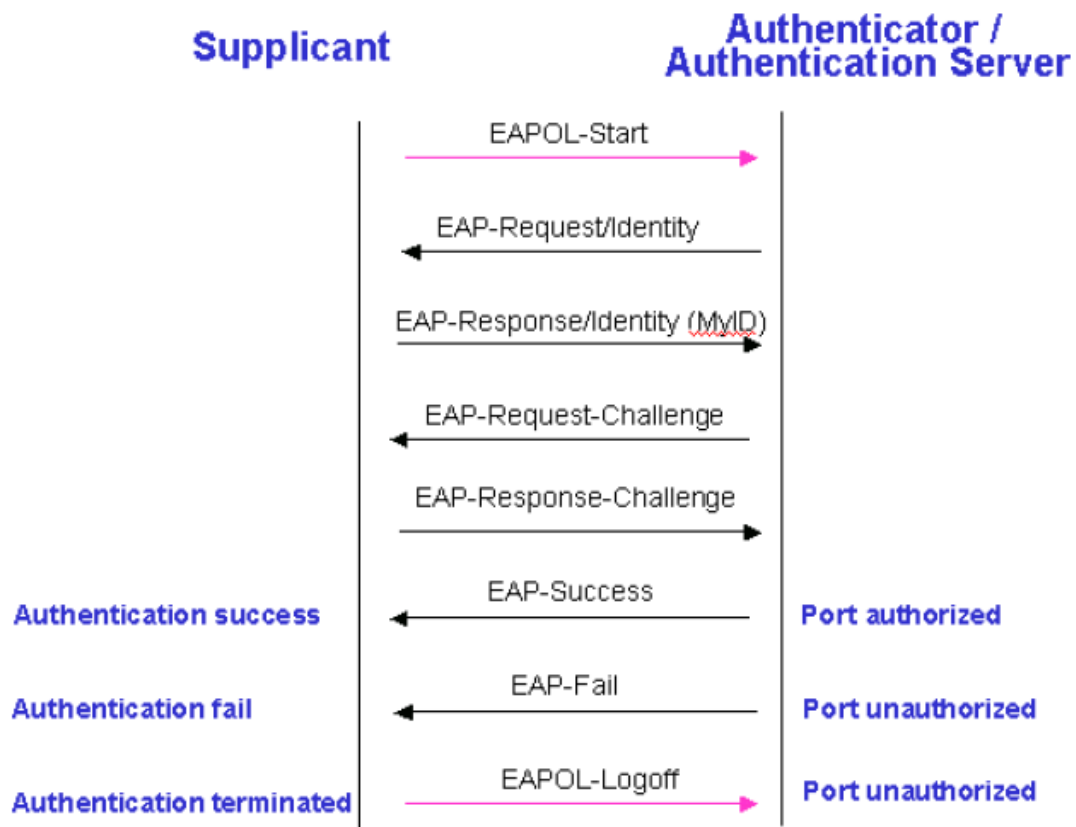


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When the supplicant receives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

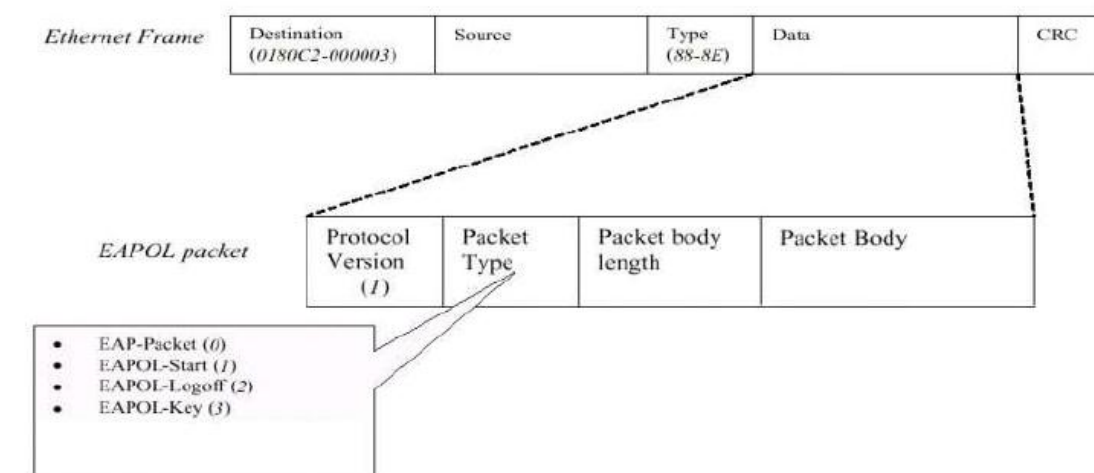
EAPOL Exchange between 802.1X Authenticator and Supplicant

The authenticator or supplicant can initiate the authentication. If you enable 802.1X authentication on the Wireless AP, the authenticator must initiate authentication when it determines that the Wireless link state has transited 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 the receipt of frame, the supplicant responds with an EAP-response/identity frame.

However, if during boot-up, the supplicant does not receive an EAP-request/identity frame from the Wireless AP, the client can initiate the authentication by sending an **EAPOL-Start** frame, which prompts the switch to request the supplicant's identity. In above case, authenticator is co-located with authentication server. When the supplicant supplies its identity, the authenticator directly exchanges the EAPOL to the supplicant until the 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 the wireless access any more, it sends an **EAPOL-Logoff** packet to terminate its 802.1X session and the port state will become unauthorized. The following figure displays 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 as follows:



- EAP-Packet: Both the supplicant and authenticator send this packet when the 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 the TLS authentication method. The Wireless AP uses this packet to send the calculated WEP key to the supplicant after the TLS negotiation has been completed between the supplicant and RADIUS server.

Wi-Fi Protected Access Introduction

The Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WAP and WEP are user authentication and improved data encryption. WAP applies the IEEE 802.1X Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You cannot use the P-660HW-Tx v2's local user database for WPA authentication purposes, since the local user database uses the MD5 EAP which cannot generate keys.

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check and IEEE 802.1x. Temporal Key Integrity Protocol uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extend initialization vector (IV) with sequencing rules and a re-keying mechanism.

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

Brief in WPA2

WPA2 (Wi-Fi Protected Access 2) is the Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA2 implements the National Institute of Standards and Technology (NIST) which security is a higher level than WPA, because it brings AES-based algorithm and Cipher Block Chaining Message Authentication Code Protocol (CCMP) in it and offers stronger encryption than WPA uses (TKIP). WPA2 encryption keys that are used for each client on the network are unique and specific to that client. Eventually, each packet which is sent over the air is encrypted with a unique key. The higher security is enhanced with the use of a new and unique encryption key because there is no key reuse.

WPA & WPA2

Both WPA & WPA2 offer a high level security for end users and administrators, which utilizes EAP (Extensible authentication Protocol) for authentication, both of them all support Personal and Enterprise mode. Because WPA2 provides a stronger encryption mechanism through AES (Advanced Encryption Standard), WPA2's level and standard is a requirement for some corporate and government users.

Wireless Configuration

Activate the WLAN interface of the LTE5121 and connect the notebook (802.11bg wireless NIC required) under the WPA-PSK security mode.

a. Wireless Setup.

1. Go to **Network Setting > Wireless > General**.
2. Check the Enable Wireless LAN box.
3. Enter the Network Name (SSID), e.g. "Test_01".

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless Network Setup

Wireless : ☒ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID):

☐ Hide SSID

BSSID : 02:13:49:11:66:8c

Mode Select : 802.11bg

Channel Selection : Auto

Operating Channel : 7

Security Level

4. Select the Security Mode, e.g. "WPA-PSK".

5. Enter the Pre-Shared Key, e.g. "njdrhwceiq".

6. Click Apply.

View all the available wireless networks on your notebook (802.11bg wireless NIC required):

Channel Selection : Auto

Operating Channel : 7

Security Level

☐ No Security
 ☐ Basic
 ☒ More Secure (Recommended)

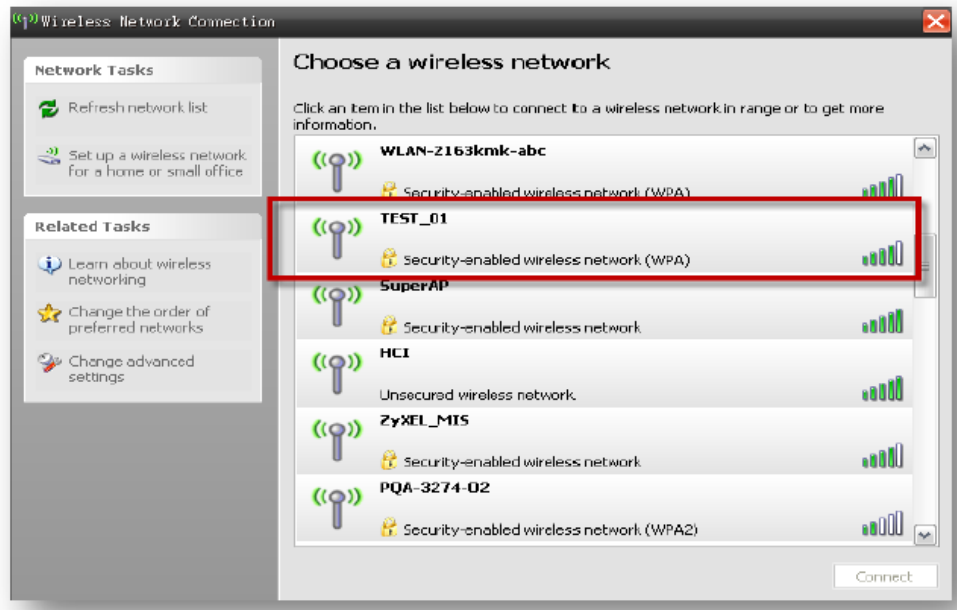
☐ No Security
 ☐ Basic
 ☒ More Secure (Recommended)

Security Mode : WPA-PSK

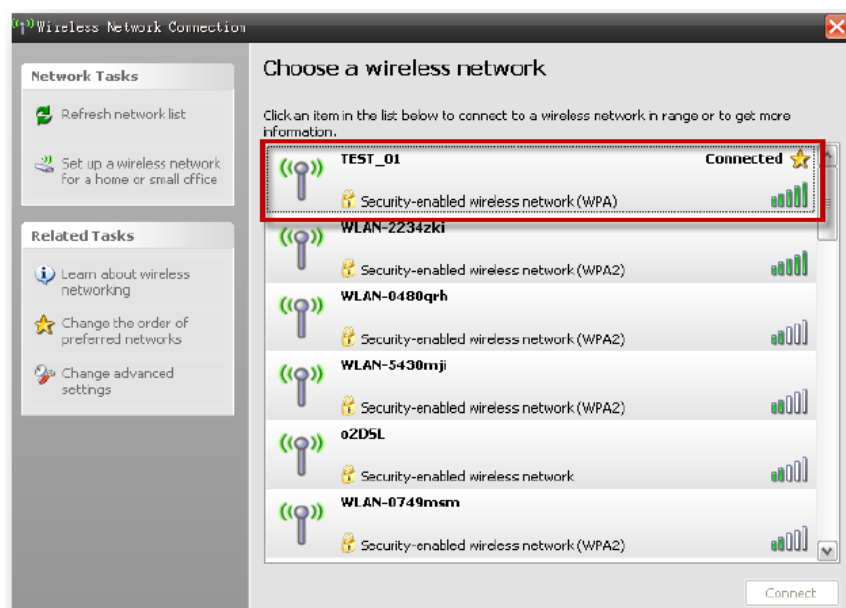
Enter 8-63 characters (a-z, A-Z, and 0-9) or 64 hexadecimal digits (a-f and 0-9). Spaces and underscores are not allowed.

Pre-Shared Key : njdrhwceiq [more...](#)

View all the available wireless networks on your notebook (802.11bg wireless NIC required):



Enter the WPA-PSK pre-shared key.



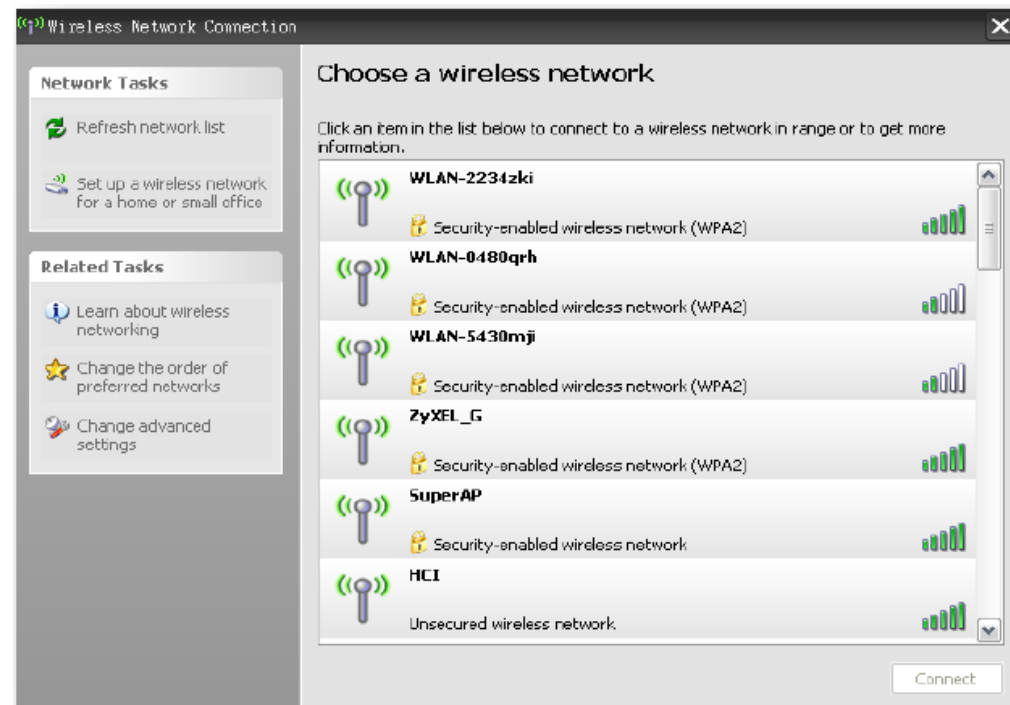
We can see that the notebook is now connected to the WLAN interface of the LTE5121.

b. Wireless Setup – Hiding the SSID.

1. Go to **Network Setting > Wireless LAN > General**.
2. Check the **Enable Wireless LAN** box.
3. Enter the **Wireless Network Name (SSID)**, e.g. “TEST_01”.
4. Check the **Hide SSID** box.
5. Select the **Security Mode**, e.g. “WPA2-PSK”.
6. Enter the **Pre-Shared Key**, e.g. “RKW7ENKNM49VW”.
7. Click **Apply**.

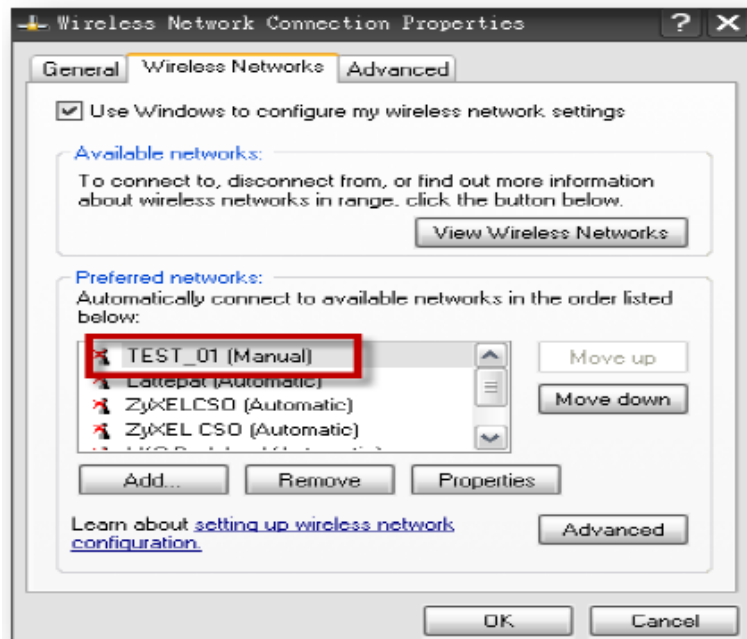


View all the available wireless networks on your notebook:

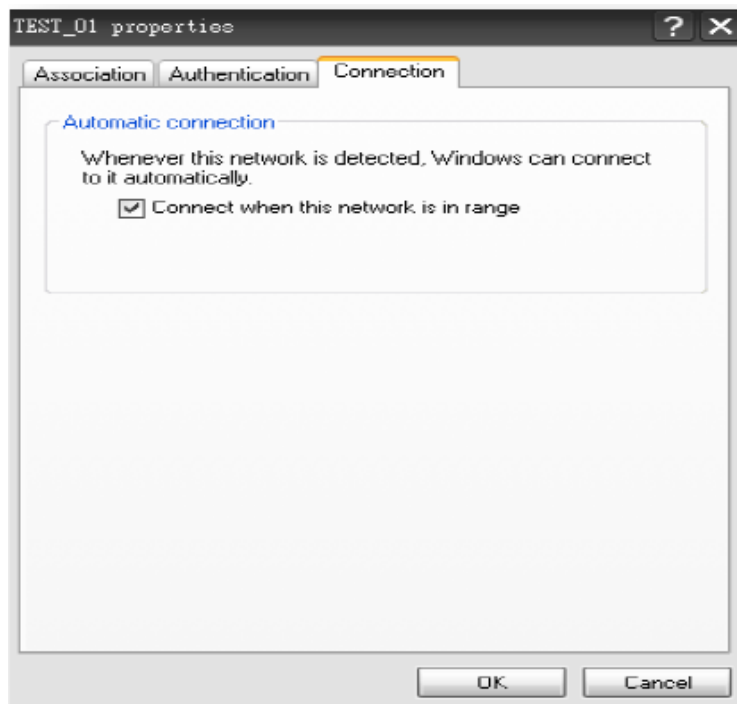


As we can see, we cannot find the SSID “TEST_01”.

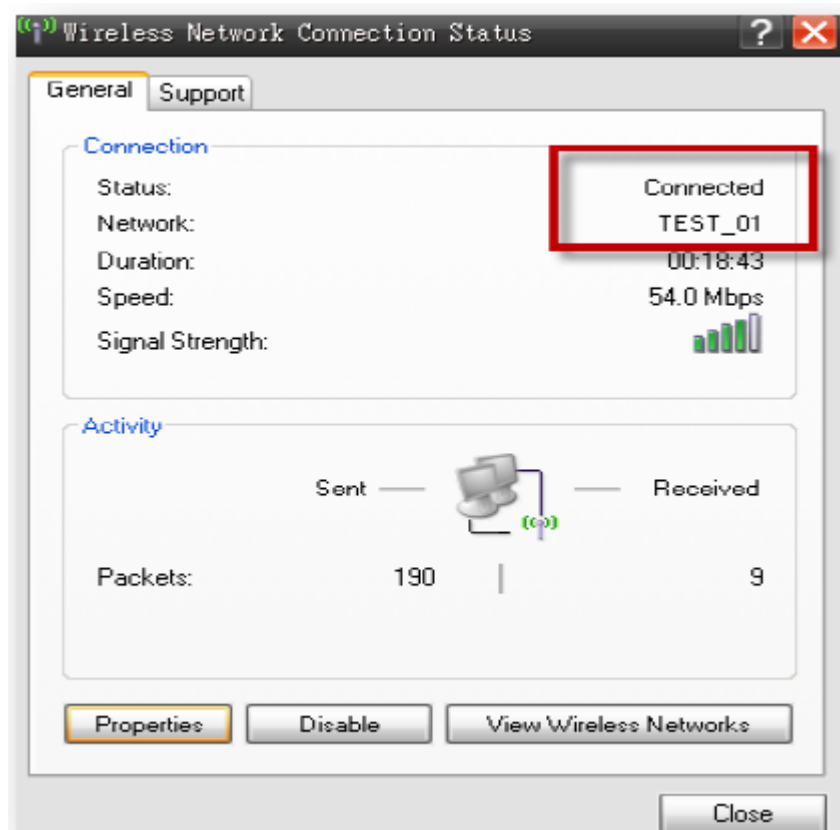
To connect to “TEST_01”, we need to configure the “Wireless Network Connection Properties” of the notebook WLAN interface:



Go to the “Connection” tab and check “Connect when this network is in range” checkbox.



We can then see the notebook connected to the “TEST_01”, even though the SSID is not displayed in the broadcast network list.



WPS Application Notes

What is WPS?

Wi-Fi Protected Setup (WPS) is a standard created by the Wi-Fi Alliance for easy and secure establishment of a wireless home/office network. The goal of the WPS protocol is to simplify the process for configuring the security of the wireless network, and thus received the name **Wi-Fi Protected Setup**.

There are several different methods defined in WPS to simplify the process of configuration. LTE5121 supports two of those methods, which are the PIN Method and the PBC Method.

PIN Method:

A PIN (Personal Identification Number) has to be read from either a sticker on the new wireless client device or a display, and entered at either the wireless access point (AP) or a Registrar of the network.

PBC Method:

A simple action of “pushing a button” suffices to activate the security of the wireless network and at the same time allow a client to subscribe to it.

WPS configuration

a. WPS Setup

1. Go to **Network Setting > Wireless > WPS**.
2. Check the “**Enable**” box for WPS.
3. Click Apply.

Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS.

General

WPS: ☒ Enable ☐ Disable

Add a new device with WPS Method

 Method 1 PBC	 Method 2 PIN
<p>Step 1. Click WPS button </p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>	<p>Step 1. Enter the PIN of your new wireless client device and then click Register </p> <p><input type="text" value="Enter PIN here"/></p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>

Note: You must press the other wireless device's WPS button within 2 minutes of pressing this button.

Maintenance Log

Internal Maintenance

The LTE5121 has the ability to record the events occurring in the CPE in a system log (according to the severity) and maintain this log in itself.

a. Activate the Maintenance Log.

1. Go to **Maintenance > Log setting**.
2. Select “Enable” for **Syslog Logging**.
3. Insert the parameters, for example the syslog server address.
4. Select the logging conditions according to user’s needs.
5. Click “**Apply**”

Log Setting defines which types of logs and which log levels you want to record. If you have a LAN client on your network that is running a syslog utility, you can also save the log files there by enabling Syslog Logging and enter the IP address of that LAN client.

Syslog Setting

Syslog Logging: ☒ Enable ☐ Disable

Syslog Server: 59.124.163.147 (IP Address)

UDP Port: 514 (Server Port)

Active Log and Select Level

Log Category	Log Level
VoIP	ALL
<input type="checkbox"/> VoIP-Call Statistics	ALL
<input checked="" type="checkbox"/> VoIP-SIP Call Signaling	ALL
<input checked="" type="checkbox"/> VoIP-SIP Registrations	ALL
<input checked="" type="checkbox"/> VoIP-Phone Event	ALL
<input checked="" type="checkbox"/> VoIP-Misc	ALL
System	ALL

b. View the log in the Web GUI.

1. Go to **System Monitor > Log**.

Log

Phone Log VoIP Call History

VoIP activities will be logged and displayed in the following table. You can define what type of events and its level you want to view. You can also refer to Maintenance > Log Setting to change which types of phone logs you want to record.

All Logs Level: All Refresh Clear Logs

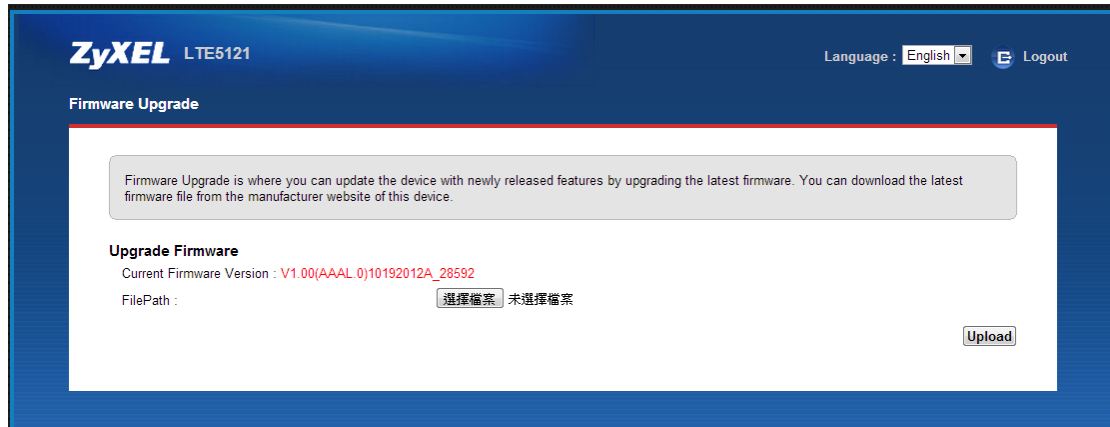
#	Time	Level	Message
1	Sep 27 12:27:07	err	SIP Registration: SIP.Changelle: Register Fail, error_cause 43 [last message repeated 1 times in 1 seconds]
2	Sep 27 12:28:57	err	SIP Registration: SIP.Changelle: Register Fail, error_cause 43
3	Sep 27 12:31:57	err	SIP Registration: SIP.Changelle: Register Fail, error_cause 43
4	Sep 27 12:34:58	err	SIP Registration: SIP.Changelle: Register Fail, error_cause 43
5	Sep 27 12:36:59	err	SIP Registration: SIP.Changelle: Register Fail, error_cause 43

Maintenance Tools

Maintenance Procedure

a. Upgrading Firmware.

1. Go to **Maintenance > Firmware Upgrade**.



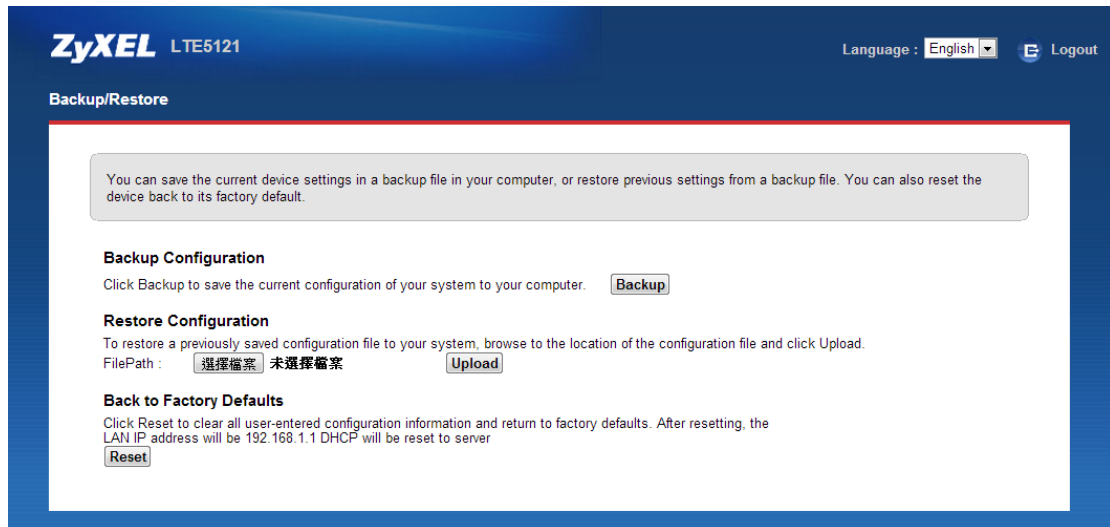
2. Click **“Browse”**.

3. Select the Firmware to upload and click **“Open”**.

4. Click **“Upload”**.

b. Backing-up the Configuration.

1. Go to **Maintenance > Backup/Restore**.



2. Click **“Backup”**.

3. Click **“Save”**.

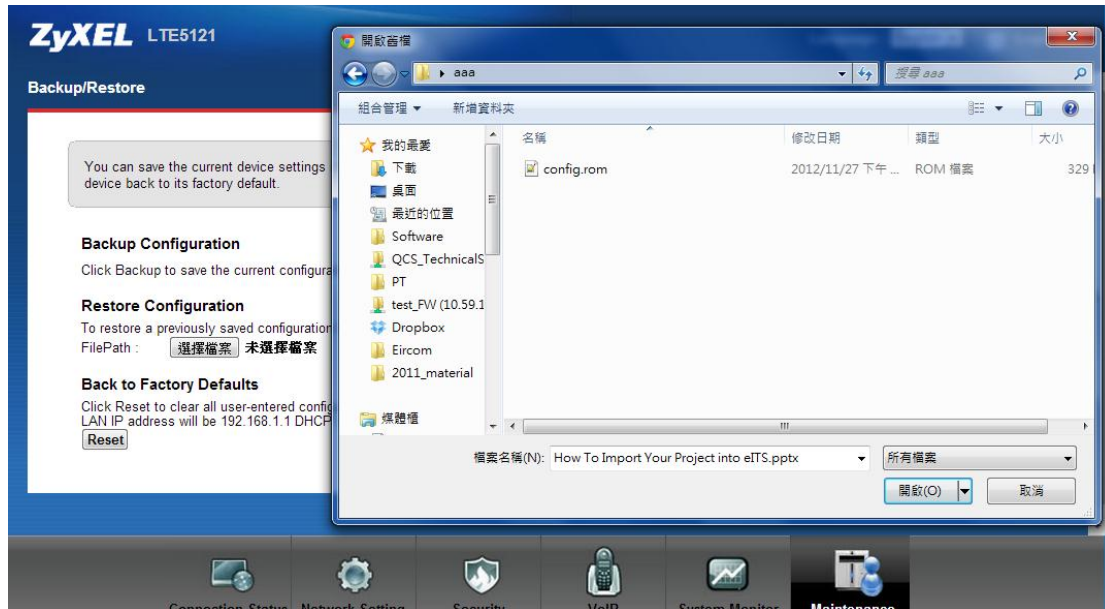
4. Select the directory to save and click **“Save”**.

c. Upload Configuration.

1. Go to **Maintenance > Tools > Configuration**.

2. Click “**Browse**”.

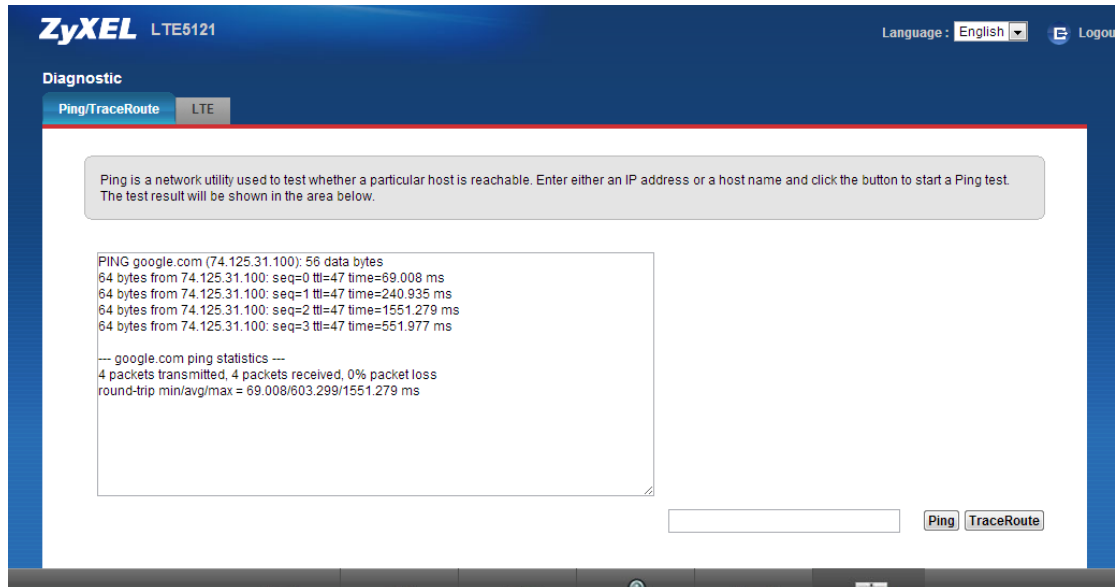
3. Select the configuration file to upload and click Open.



WAN (LTE) Connection Information

1. The best and simple way to check if your device has Internet access is to ping a public IP or domain name.

Maintenance → Diagnostic → “Ping/TraceRoute”



2. If your device does not have Internet access, you may need to check the LTE status.

Maintenance → Diagnostic → LTE Status

Maintenance → Diagnostic → LTE Service Status

Here you can check LTE information/status, including SIM card, operating frequency band, radio signal strength/quality, and device WAN IP.

ZyXEL

LTE5121

Language: English

Diagnostic

Ping/TraceRoute

LTE

3 methods are provided to test the status of LTE modem. The test results will be shown in the area below.

```

Status : UP
DeviceManufacturer : Sierra Wireless, Incorporated
DeviceModelName : MC7710
DeviceFirmwareVersion : SWI9200X_03.00.08.02AP
DeviceIMEI : 358178040089858
SIMCardIMSI : 466923102469867
ConnectionUpTime : 3989
DeviceStatus : 3G UMTS
FrequencyBand : WCDMA 2100
ServiceProvider : Chunghwa Telecom
SignalStrength : -61 dBm
SignalQuality : HIGH
Temperature : 42
ValidErrorPINTimes : 3
ValidErrorPUKTimes : 10

```

LTE Status

LTE Service Status

Reset LTE modem

Connection Status

Network Setting

Security

VoIP

System Monitor

Maintenance

ZyXEL

LTE5121

Language: E

Diagnostic

Ping/TraceRoute

LTE

3 methods are provided to test the status of LTE modem. The test results will be shown in the area below.

```

SignalQuality : HIGH
Temperature : 42
ValidErrorPINTimes : 3
ValidErrorPUKTimes : 10
CurrentRS : RS_READY
LTE bw : UNKNOWN
LTE Rx chan : N/A
LTE Tx chan : N/A
RSRP : N/A
RSRQ : N/A
SINR : N/A
Tx Power : N/A
TAC : 0 (N/A)
Cell ID : 161F9C0 (23198144)

```

LTE Status

LTE Service Status

Reset LTE modem

Connection Status

Network Setting

Security

VoIP

System Monitor

Maintenance

Diagnostic

Ping/TraceRoute

LTE

3 methods are provided to test the status of LTE modem. The test results will be shown in the area below.

```
1: [CONN] 1 [TYPE] IP [APN] [IF] usb0 [IP] 111.81.182.50 [MASK] 255.255.255.255 [GW]
111.81.182.50 [DNS1] 168.95.1.1 [DNS2] 168.95.192.1
2: [CONN] 0 [TYPE] IP [APN] [IF] [IP] [MASK] [GW] [DNS1] [DNS2]
```

LTE Status

LTE Service Status

Reset LTE modem

Product FAQ

Why do I need to use LTE5121?

LTE5121 provides a high speed wireless Internet access solution for home users, no more Ethernet cable or DSL cable are required, all you need is a SIM card (which is obtained from ISP). LTE5121 serves multiple purposes, Internet access, VoIP client, File Sharing, Media Server, and Print Server.

What is APN?

APN (Access Point Name) is a unique string which indicates the UMTS/LTE network. An APN is required for stations to enter the UMTS/LTE network (Internet).

Which Internet Applications can I use with the device?

Most common applications include MIRC, PPTP, ICQ, Cu-SeeMe, NetMeeting, RealPlayer, Quake, QuakeII, QuakeIII, StarCraft, & Quick Time.

How can I configure the device?

- a. Telnet remote management-driven user interface for easy remote management
- b. Web browser - embedded web server for easy configuration

What can we do with the device?

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

Does the device support dynamic IP addressing?

The device supports 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 Device works like an intelligent router that routes between the virtual IP and the real IP.

How does e-mail work through the device?

Depending on the email system used by your company, you may need to connect to an email server at your office or your ISP, or alternatively to a public email service provider. Customers with a public static IP and a domain name may choose to host their own email server connected to the local LAN. In case your company's email is 'xxx@mycompany.com', your users may need to connect to a local email server, which then transmits all email on their behalf through the office internet connection.

Companies that use email hosting services at the ISP or another provider may require their users to download and send email directly through a server on the Internet. Individual users will then need to utilize the office internet connection to check their individual email accounts. This kind of setup doesn't require a public static IP address from the ISP.

What DHCP capability does the device support?

The device supports DHCP client (Ethernet encaps) on the WAN port and DHCP server on the LAN port. The device's DHCP client allows it to get the Internet IP address

from ISP automatically if your ISP uses DHCP as a method to assign IP address. The device's internal DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

How do I use the reset button, and what parameters will be reset by the reset button?

You can use a blunt pointed object and insert it into the small reset button hole beside the power connector. Press down the reset button and hold it down for approximately 5 seconds, the unit will be reset. When the reset button is pressed, all the device parameters will be reset back to factory defaults, including password and IP address. The default IP address is 192.168.1.1, password 1234.

What network interface does the new device series support?

The new device series supports auto MDX/MDIX 10/100M Ethernet LAN port to connect to the computer or Switch on LAN.

How does the device support TFTP?

In addition to the direct console port connection, the device supports uploading/download of firmware and configuration file using TFTP (Trivial File Transfer Protocol) over LAN.

Can the device support TFTP over WAN?

Although TFTP should work over WAN as well, it is not recommended because of the potential data corruption problems.

When do I need NAT?

- a. To make a local server accessible from the Internet
When NAT is enabled the local computers are not accessible from outside. You can use Multi-NAT to make an internal server accessible from outside.
- b. Support Non-NAT Friendly Applications
Some servers providing Internet applications such as some mIRC servers do not allow users to log in using the same IP address. Thus, users on the same network cannot log in to the same server simultaneously.

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 to a TCP/IP client by a server. In this case, the device is a BOOTP/DHCP server. Windows 95 and newer 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 for an account from one of several free Web servers such as WWW.DYNDNS.ORG.

Without DDNS, we need to tell the users to use the WAN IP of the LTE5121 to reach our internal servers. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the device, you apply for a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users will then be able to access the web server using the URL www.zyxel.com.tw regardless of the WAN IP of the LTE5121.

When the ISP assigns the device (LTE5121) a new IP, the device updates this IP to the 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) can be used to access your server from the Internet.

When do I need DDNS service?

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

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 air. Typical bit-rates are 11 Mbps and 54 Mbps, 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. APs 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 cables through walls and ceilings.

c. Installation Flexibility:

Wireless technology allows the network to go where a 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 infra-structure 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 relatively slower than wired LAN. The most popular wired LAN is operated in 100 Mbps, which is several times of that of Wireless LAN (10-54 Mbps). A faster wired LAN standard (1000 Mbps), which is 10 times faster, is becoming popular as well. The setup cost of Wireless LAN is relatively high because the equipment cost including access points and Wireless LAN cards is higher than hubs/switches 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 proliferate, this will create additional security risk for remote users if not properly protected.

What is an Access Point?

The AP (access point also known as a base station) is a wireless server with a wired Ethernet connection that broadcasts information using radio signals with an antenna. An 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/company 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 manufacturers' wireless LAN devices can communicate with each other. 802.11 provides 1 or 2 Mbps transmission rates 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 11 Mbps in the 2.4 GHz 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 1 Mbps.

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 is the second revision of 802.11 that operates in the unlicensed 5 GHz band and allows transmission rates of up to 54 Mbps. 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 can 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 utilizes 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.

What is 802.11n?

802.11n supports frequencies in both 2.4GHz and 5 GHz bands and its data rate ranges from 54 Mbit/s up to 600 Mbit/s in theory; using the 802.11n Channel Doubling technology which can double the bandwidth from 20 MHz to 40 MHz and effectively doubles data rates and throughput. 802.11n adds MIMO feature, which uses multiple transmission and reception antennas to allow higher raw data rate, and resolves more information than possible using a single antenna. It also uses the “Alamouti coding” coding schemes to increase transmission range.

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 802.11 compatible products.

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 2.4 GHz Band?

Various spread spectrum radio communication applications use the 2.4 GHz band. This includes WLAN systems (not necessarily of the IEEE 802.11 type), 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 same 2.4-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 reinforcement used.

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

Factors of interference:

1. Obstacles: walls, ceilings, furniture... etc.
2. Building materials: metal doors, aluminum studs.
3. Electrical devices: microwaves, monitors, electric motors.

Solution:

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

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 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 to 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 unsynchronized receiver 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 2.4 GHz or 5 GHz operation. WLAN NICs often include an internal antenna which may provide sufficient reception.

What is 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 with the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. From a security point of view, SSID 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 a mobile device must match the ESSID of the AP to communicate with the AP. The ESSID is at most a 32-character string and is case-sensitive.

How do I secure the data across an Access

Point's radio link?

Enable Wired Equivalency Protocol (WEP) or Wi-Fi Protected Access (WPA) 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 to anyone who does not have the assigned key. WEP comes in 40/64-bit and 104/128-bit encryption key lengths. Note, WEP has been shown to have fundamental flaws in its key generation process.

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.

Are different WEP key lengths compatible?

128-bit WEP will not communicate with 64-bit WEP or 256-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 with the network to see the SSID.

What are Insertion Attacks?

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

What is a 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 Authentication Types?

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.

Shared 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 No Authentication required, No access allowed and Authentication required?

No authentication required—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.

No access allowed—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.

Authentication required—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.

What is WPA?

WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

What is WPA-PSK?

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

What is WPA2?

WPA2 (Wi-Fi Protected Access 2) is a successor to WPA with a higher level of security, because it brings AES-base algorithm and CCMP in it and offers stronger encryption then TKIP used in WPA. WPA2 encryption keys that are used for each client on the network are unique and specific to that client. Additionally, each packet which is sent over the air is encrypted with a unique key. The higher security is enhanced

with the use of a new and unique encryption key because there is no key reuse.