

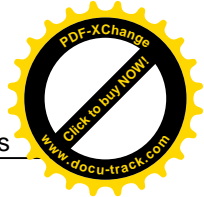
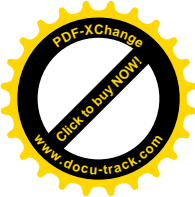
VSG1432-B101

Support Notes

August 2010

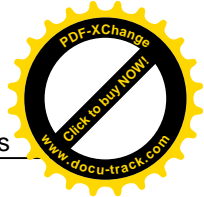
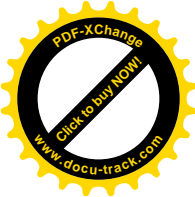
Edition 1.0



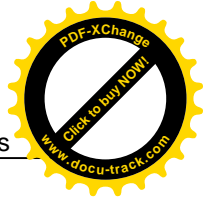
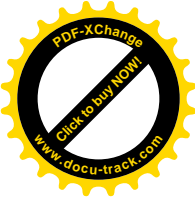


Index

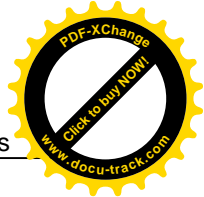
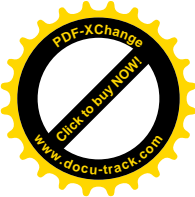
General Application Notes	6
Why use VSG1432-B101?.....	6
Application Scenario	7
Prologue	9
Access Application Notes	11
Web GUI	11
Telnet.....	12
Broadband	13
VDSL Interface Configuration	13
WAN Configuration.....	14
Bridge Mode	14
IPoE Mode	16
PPPoE Mode	17
Ethernet Mode.....	19
IP Multicast	21
IP Multicast Introduction.....	21
IGMP Setting	22
Protocol Based Scenario	23
Environment	23
WAN Configuration	24
VLAN Based Scenario.....	28
Environment	28
WAN Configuration	29
Quality of Service.....	33
Environment	33
QoS configuration.....	34
TR069 – Remote Firmware Upgrade	38
Environment	38
TR069 Configuration	39
ACS server (Vantage Access 3.0)	40
NAT Port Forwarding	41
NAT/Multi-NAT Introduction.....	41
Environment	44
Port Forwarding Configuration	45
DMZ Host Configuration.....	48
LAN Connection	49



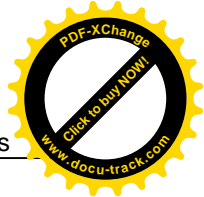
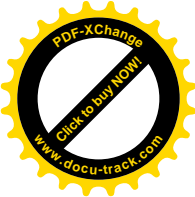
IP Alias Introduction	49
IP Alias Configuration	50
Client List Configuration	50
Using Universal Plug n Play (UPnP)	52
Universal Plug n Play (UPnP) Configuration	55
Maintenance Log	56
Internal Maintenance.....	56
Remote Maintenance.....	58
Maintenance Tool	59
Maintenance Procedure	59
Wireless Application Notes	63
Wireless Introduction.....	63
Wireless Configuration.....	72
WPS Application Notes	83
What is WPS?.....	83
WPS configuration	84
Product FAQ.....	86
Will the device work with my Internet connection?	86
Why do I need to use VSG1432-B101?.....	86
What is PPPoE?	86
Does the device support PPPoE?.....	86
How do I know I am using PPPoE?.....	87
Why does my provider use PPPoE?.....	87
Which Internet Applications can I use with the device?	87
How can I configure the device?	87
What network interface does the device support?	87
What can we do with the device?	87
Does device support dynamic IP addressing?	87
What is the difference between the internal IP and the real IP from my ISP?	88
How does e-mail work through the device?.....	88
Is it possible to access a server running behind SUA from the outside Internet? If possible, how?	88
What DHCP capability does the device support?.....	89
How do I used the reset button, more over what field of parameter will be reset by reset button?.....	89
What network interface does the new device series support?.....	89
How does the device support TFTP?.....	89



Can the device support TFTP over WAN?	89
How fast can the data go?	90
What is Multi-NAT?	90
When do I need Multi-NAT?	91
What IP/Port mapping does Multi-NAT support?	91
What is the difference between SUA and Multi-NAT?	92
What is BOOTP/DHCP?	93
What is DDNS?	93
When do I need DDNS service?	93
Wireless FAQ	94
What is a Wireless LAN?	94
What are the advantages of Wireless LANs?	94
What are the disadvantages of Wireless LANs?	95
Where can you find wireless 802.11 networks?	95
What is an Access Point?	95
What is IEEE 802.11?	95
What is 802.11b?	95
How fast is 802.11b?	96
What is 802.11a?	96
What is 802.11g?	96
Is it possible to use products from a variety of vendors?	96
What is Wi-Fi?	97
What types of devices use the 2.4GHz Band?	97
Does the 802.11 interfere with Bluetooth devices?	97
Can radio signals pass through walls?	97
What are potential factors that may causes interference among WLAN products?	98
What's the difference between a WLAN and a WWAN?	98
What is Ad Hoc mode?	98
What is Infrastructure mode?	98
How many Access Points are required in a given area?	99
What is Direct-Sequence Spread Spectrum Technology – (DSSS)?	99
What is Frequency-hopping Spread Spectrum Technology – (FHSS)?	99
Do I need the same kind of antenna on both sides of a link?	99
Why the 2.4 Ghz Frequency range?	99
What is Server Set ID (SSID)?	100
What is an ESSID?	100
How do I secure the data across an Access Point's radio link?	100



What is WEP?.....	100
What is the difference between 40-bit and 64-bit WEP?.....	100
What is a WEP key?	101
A WEP key is a user defined string of characters used to encrypt and decrypt data?.....	101
Can the SSID be encrypted?.....	101
By turning off the broadcast of SSID, can someone still sniff the SSID? .	101
What are Insertion Attacks?	101
What is Wireless Sniffer?.....	101
What is the difference between Open System and Shared Key of Authentication Type?.....	102
What is 802.1x?	102
What is the difference between No authentication required, No access allowed and Authentication required?	102
What is AAA?	103
What is RADIUS?	103
What is WPA?	103
What is WPA-PSK?	103
Trouble Shooting	104
How to enter the “Shell mode”	104
CPU usage	104
Memory usage	105
Current processes	106
NAT session table	107
IGMP table	108
Packets statistics	109
Physical layer statistics	110
CLI Command List	111



General Application Notes

Why use VSG1432-B101?

- **High Speed Internet Access**

The VSG1432-B101 is a VDSL\ADSL\Ethernet gateway supporting the downstream transmission up to 1Gbps and upstream transmission up to 1Gbps.

- **Quality of Service (QoS)**

The VSG1432-B101 with Quality of Service features ensures that the Triple Play Service keeps the high quality delivery in high speed Internet access.

- **PPP over Ethernet**

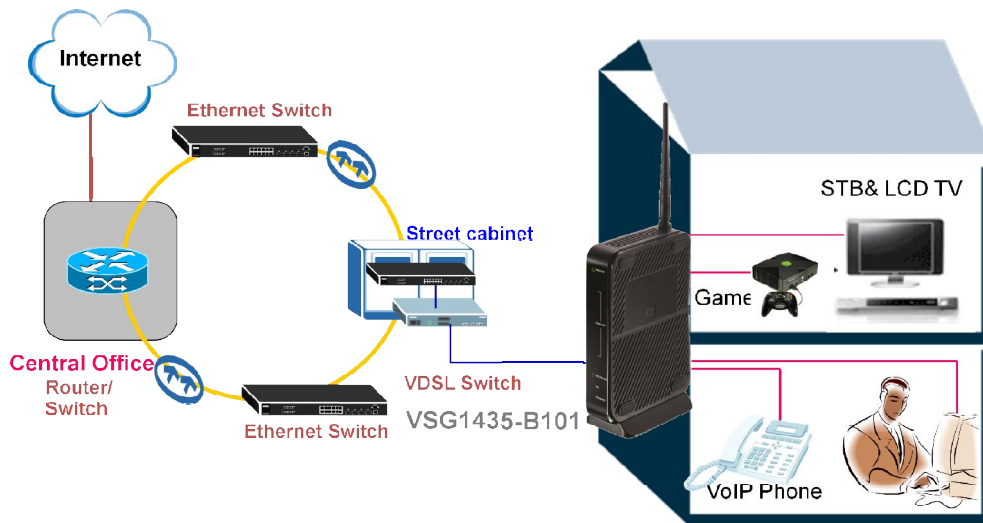
Since the PPPoE will benefit both Telco and ISP, the VSG1432-B101 shall implement this feature and be tested well with the PPPoE servers.

- **Multi-NAT**

The NAT provides system administrators an easy solution to create a private IP network for the security and IP management. Powered by NAT technology, the VSG1432-B101 supports the complete NAT mapping and most popular Internet multimedia applications, such as NetMeeting, MSN Messenger, Skype, ICQ, IPTV, QuickTime, Real Player (RSP/RTSP), VoIP SIP ALG, etc.

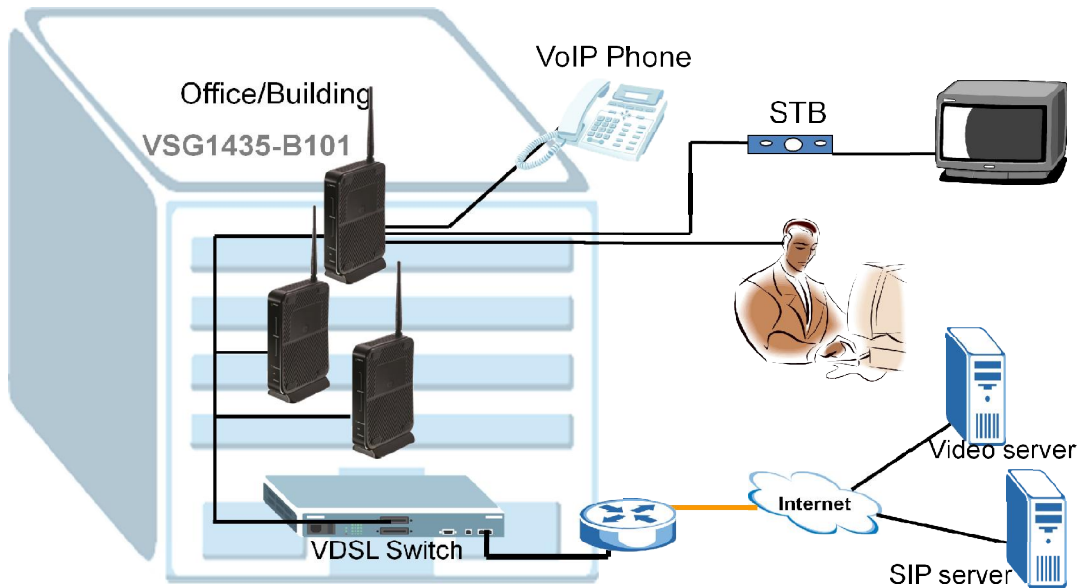
Application Scenario

FTTx - FTTC Solution

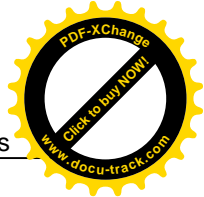
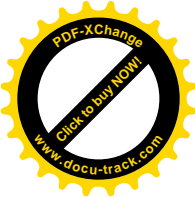


A typical scenario is used with VSG1432-B101 in a FTTC (Fiber to the Curb) solution. The VSG1432-B101 serves as a home gateway, providing the high speed INTERNET service and High Quality IPTV service. The COE (VDSL switch) is located in a street cabinet, providing a high speed service within a 600 feet range, assuring the bandwidth reaching up to 100/45Mbps (Downstream/Upstream) at maximum.

FTTx – FTTB Solution



An often seen scenario is used with VSG1432-B101 in a FTTB (Fiber to the Building) solution. The VSG1432-B101 serves as a home gateway, providing the high speed INTERNET service, High Quality IPTV service and VoIP service. The COE (VDSL switch) is located inside the cabinet of building, providing a high speed service covering the whole apartment, assuring the bandwidth reaching up to 100/45Mbps (Downstream/Upstream) at maximum.



Prologue

- Before we begin.

The device is shipped with the following factory defaults:

1. IP address = 192.168.1.1, subnet mask = 255.255.255.0 (24 bits)
2. DHCP server enabled with IP pool starting from 192.168.1.2
3. Default username/password = admin/1234

- Setting up the PC (Windows OS)

1. Ethernet Connection

- All PCs must have an Ethernet adapter card installed

2. TCP/IP Installation

You must first install the TCP/IP software on each PC before you can use it for the Internet access. If you have already installed the 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**.

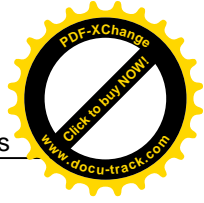
3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

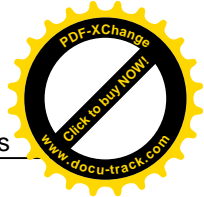
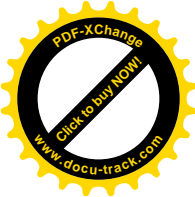
- In the **Control Panel/Network** window, click the **TCP/IP** entry to select it and click **Properties** button.
- In the **TCP/IP** Properties window, select **obtain an IP address automatically**.

Note: Do not assign the 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 that your Device is powered on before answering “Yes” to the prompt. Repeat the aforementioned steps for each Windows PC on your network.



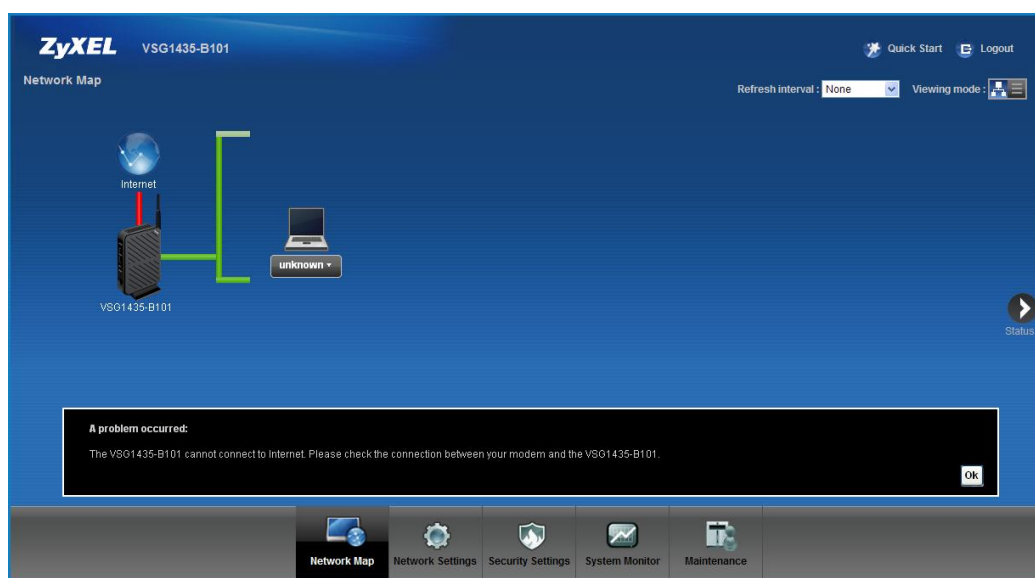
Access Application Notes

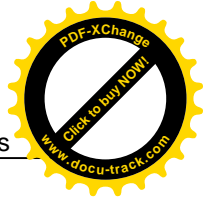
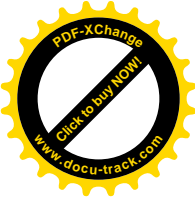
Web GUI

The following procedure is for the most typical usage of device using a Browser. The device supports the embedded Web server that allows you to use Web browser to configure it. Before configuring the router using Browser, please be sure there is no Telnet or Console login.

a. Login the VSG1432-B101 via Web GUI.

1. Set up your PC/NB IP address to be a DHCP client.
2. Connect to a LAN port of VSG1432-B101 via RJ45 Ethernet cable and open your IE browser.
3. The default IP of VSG1432-B101 is 192.168.1.1 username/password = admin/1234.





Telnet

Telnet is also a common way to configure the device, but we have to use CLI commands which may not be quick-to-learn. The list of the commonly used CLI commands is provided at the end of this document.

b. Login the VSG1432-B101 via Telnet.

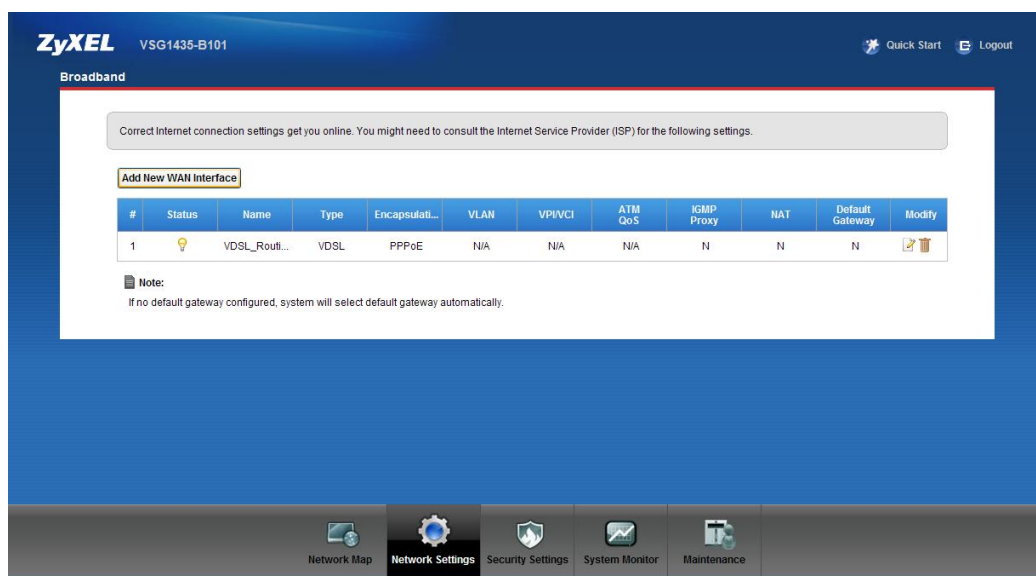
1. Set up your PC/NB IP address to be a DHCP client.
2. Connect to a LAN port of VSG1432-B101 via RJ45 Ethernet cable and open your Hyper Terminal software (capable of using TELNET).
3. The default IP of VSG1432-B101 is 192.168.1.1 username/password = admin/1234.
4. Type the command line "atsh" to display the basic information of device.

```
C:\> Telnet 192.168.1.1
ZyXEL VSG1435-B101
Login: admin
Password:
Last login from: 192.168.1.66
> sys atsh
ZLD      Version      : U1.10<TUB.0>b6
Bootbase Version    : U1.32 ; 09/13/2010 22:25:16
Vendor Name       : ZyXEL Communications Corp.
Product Model      : DSL-491HNUP-B1B
Serial Number      : S090Y000000000
First MAC Address   : 021018010000
Last MAC Address    : 021018010007
MAC Address Quantity : 08
Default Country Code : FF
Boot Module Debug Flag : 01
RootFS      Checksum   : 05eb783b
Kernel      Checksum   : 458a61ba
RomFile     Checksum   : a6c85164
ImageDefaultChecksum : ffffffff
Main Feature Bits   : 00
Other Feature Bits   :
      5a 59 40 05 00 00 00 00-00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
>
```

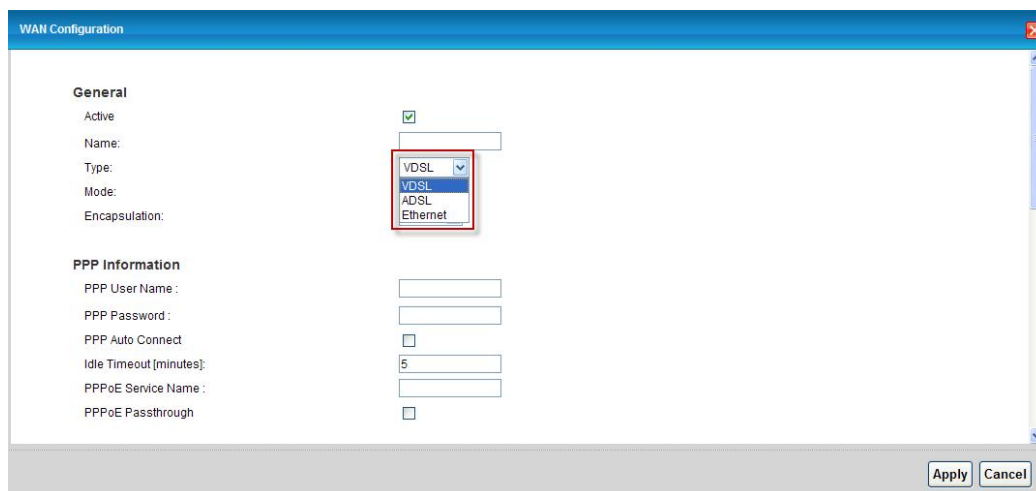
Broadband

VDSL Interface Configuration

1. Click **Network Settings > Broadband** to modify the type of the WAN Layer 2 Interface.



2. There are three Interfaces support for VSG1432-B101.
3. In the Broadband Interface Configuration page, there are three types: **VDSL Mode**, **ADSL Mode** and **Ethernet Mode**.



WAN Configuration

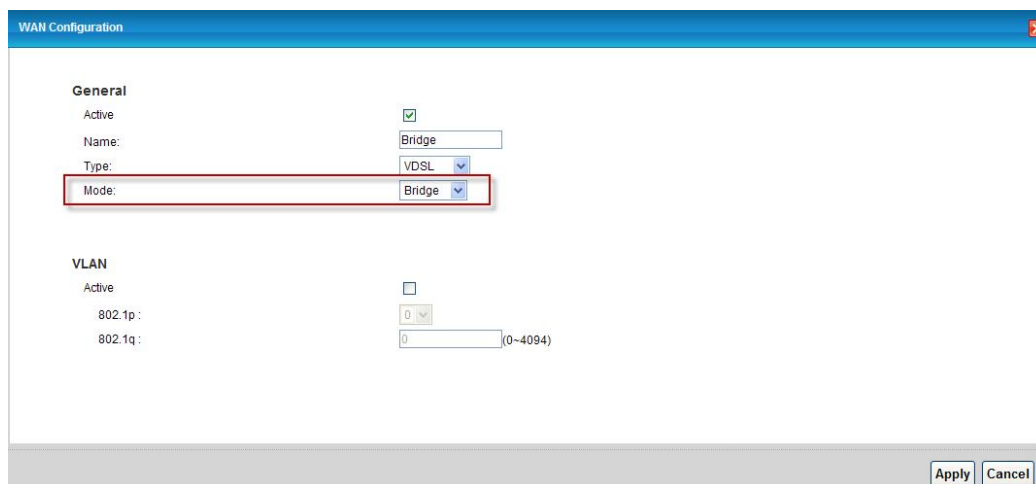
Bridge Mode

Scenario:

The VSG1432-B101 is a CPE bridge.

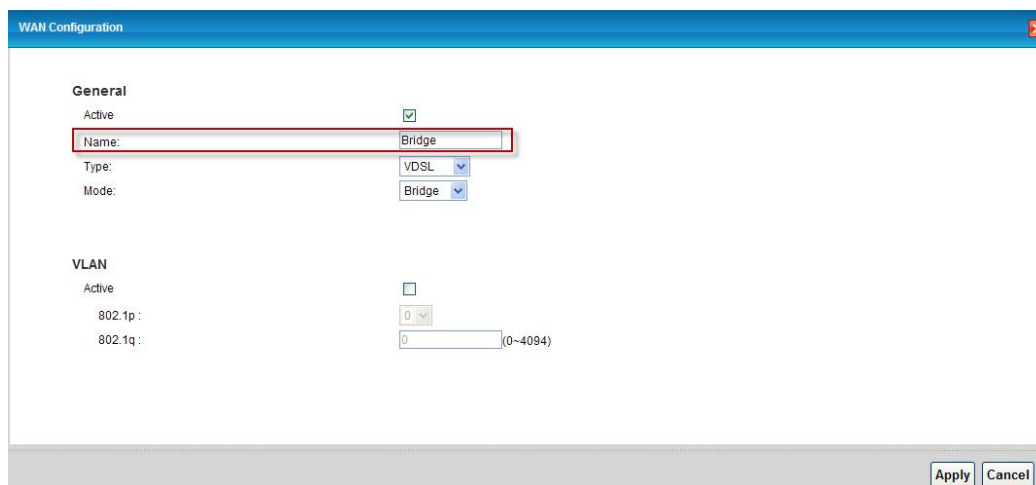
a. Bridge Mode

1. Go to **Network Settings > Broadband > Add New WAN Interface**.
2. Click modify icon to modify the WAN service of VSG1432-B101 to bridge mode.

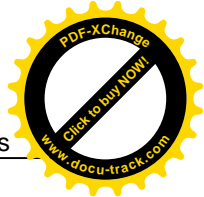
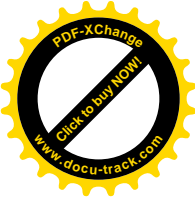


The image shows the 'WAN Configuration' dialog box. Under the 'General' section, the 'Active' checkbox is checked. The 'Name' field is set to 'Bridge'. The 'Type' dropdown is set to 'VDSL'. The 'Mode' dropdown is highlighted with a red box and is set to 'Bridge'. Under the 'VLAN' section, the 'Active' checkbox is unchecked. The '802.1p' field is set to '0' and the '802.1q' field is set to '0' with a range of '(0~4094)'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

3. Select the WAN service type to be **"Bridging"**. Also you want to enter the Name.



The image shows the 'WAN Configuration' dialog box. Under the 'General' section, the 'Active' checkbox is checked. The 'Name' field is highlighted with a red box and is set to 'Bridge'. The 'Type' dropdown is set to 'VDSL'. The 'Mode' dropdown is set to 'Bridge'. Under the 'VLAN' section, the 'Active' checkbox is unchecked. The '802.1p' field is set to '0' and the '802.1q' field is set to '0' with a range of '(0~4094)'. At the bottom right, there are 'Apply' and 'Cancel' buttons.



4. Click **Apply** to Save. The summary will be showed on the Broadband page that includes all related configuration parameters.

Broadband

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

Add New WAN Interface

#	Status	Name	Type	Encapsulati...	VLAN	VP/VC1	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		Bridge	VDSL	Bridge	N/A	N/A	N/A	N	N	N	

Note:
If no default gateway configured, system will select default gateway automatically.

IPoE Mode

Scenario:

The VSG1432-B101 is a DHCP client in routing mode.

b. IPoE Mode

1. Go to **Network Settings > Broadband**.
2. Click modify icon to modify the WAN service type of VSG1432-B101.
3. Select the Encapsulation to be “**IPoE**”. Also you want to enter the Name.

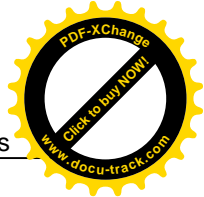
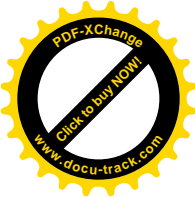
The image shows the 'WAN Configuration' dialog box. Under the 'General' tab, the 'Active' checkbox is checked. The 'Name' field is set to 'IPoE_test'. The 'Type' is set to 'VDSL', 'Mode' is 'Routing', and 'Encapsulation' is 'IPoE'. Under the 'IP Address' section, 'Obtain an IP Address Automatically' is selected. The 'Static IP Address' section is also visible with fields for IP Address, Subnet Mask, and Gateway IP address, all currently set to 0.0.0.0. 'Apply' and 'Cancel' buttons are at the bottom right.

4. Click Apply button to save and then review all WAN setup parameters to make sure all related settings are correct.

The image shows the 'Broadband' configuration page. At the top, a message states: 'Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.' Below this is a button 'Add New WAN Interface'. A table lists the WAN interfaces:

#	Status	Name	Type	Encapsulati...	VLAN	VP/VC	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		IPoE_test	VDSL	IPoE	N/A	N/A	N/A	N	N	N	

Below the table, a 'Note' states: 'If no default gateway configured, system will select default gateway automatically.'



PPPoE Mode

Scenario:

The VSG1432-B101 is a PPPoE client.

c. PPPoE Mode

1. Go to **Network Settings > Broadband**.
2. Click modify icon to modify the WAN service type of VSG1432-B101.
3. Select **Encapsulation** to be “**PPPoE**”. Also you want to enter the Name.

The screenshot shows the 'WAN Configuration' dialog box with the following settings:

General	
Active	<input checked="" type="checkbox"/>
Name:	PPPoE_test
Type:	VDSL
Mode:	Routing
Encapsulation:	PPPoE

PPP Information	
PPP User Name :	test
PPP Password :	•••••
PPP Auto Connect	<input type="checkbox"/>
Idle Timeout (minutes):	5
PPPoE Service Name :	
PPPoE Passthrough	<input type="checkbox"/>

Buttons: Apply, Cancel

4. Enter the **PPP Username**, e.g. "test". Enter the **PPP Password**, e.g. "1234".

The image shows the 'WAN Configuration' window. The 'General' tab is active, showing the following settings:

- Active: ☒
- Name: PPPoE_test
- Type: VDSL
- Mode: Routing
- Encapsulation: PPPoE

The 'PPP Information' tab is also visible, showing the following settings:

- PPP User Name: test
- PPP Password: ****
- PPP Auto Connect: ☐
- Idle Timeout (minutes): 5
- PPPoE Service Name:
- PPPoE Passthrough: ☐

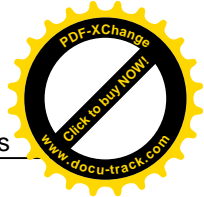
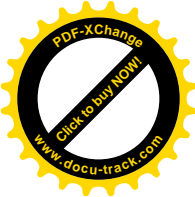
Buttons for 'Apply' and 'Cancel' are at the bottom right.

5. Click Apply button to save and then review all WAN setup parameters to make sure all related settings are correct.

The image shows the 'Broadband' window. It contains a message: "Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings." Below this is a button labeled "Add New WAN Interface".

#	Status	Name	Type	Encapsulati...	VLAN	VP/VC1	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		PPPoE_test	VDSL	PPPoE	N/A	N/A	N/A	N	N	N	

Note:
If no default gateway configured, system will select default gateway automatically.



Ethernet Mode

Scenario:

The VSG1432-B101 has more than one remote node (WAN Interface). In this case, the second WAN interface is using the “Ethernet Encapsulation” as its format for its transmission to the Central Office.

d. More than one connection

1. Go to **Network settings > Broadband**.
2. Click **Add New WAN Interface**.

Broadband

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

Add New WAN Interface

#	Status	Name	Type	Encapsulation	VLAN	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		Ethernet_test	Ethernet	Bridge	N/A	N/A	N/A	N	N	N	

Note:
If no default gateway configured, system will select default gateway automatically.

- Select the WAN service type to be **"Ethernet"**. Fill in the **802.1P priority** and **802.1Q VLAN ID** for this WAN Service. Also you want to enter the Name.

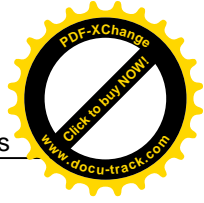
The screenshot shows the 'WAN Configuration' window. Under the 'General' tab, the 'Active' checkbox is checked. The 'Name' field contains 'Ethernet_test'. The 'Type' dropdown is set to 'Ethernet' and the 'Mode' dropdown is set to 'Bridge'. Under the 'VLAN' tab, the 'Active' checkbox is unchecked. The '802.1p' dropdown is set to '0' and the '802.1q' field contains '0' with a range '(0-4094)' indicated. At the bottom right, there are 'Apply' and 'Cancel' buttons.

- Click Apply button to save and then review all WAN setup parameters to make sure all related settings are correct.

The screenshot shows the 'Broadband' window. At the top, a message states: 'Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.' Below this is a button labeled 'Add New WAN Interface'. The main part of the window contains a table with the following data:

#	Status	Name	Type	Encapsulation	VLAN	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		Ethernet_test	Ethernet	Bridge	N/A	N/A	N/A	N	N	N	

Below the table, there is a 'Note:' section with the text: 'If no default gateway configured, system will select default gateway automatically.'



IP Multicast

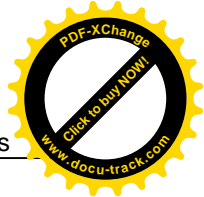
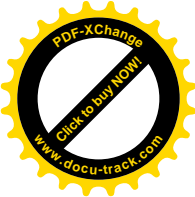
IP Multicast Introduction

- What is the IP Multicast?

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

The IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (See RFC2236). The IP hosts use the IGMP to report their multicast group membership to any immediate-neighbor multicast routers, so the multicast routers can decide if a multicast packet needs to be forwarded. At the start-up, the Prestige queries all directly connect networks to gather group membership.

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



IGMP Setting

a. IP Multicast

1. Go to **Network Settings > IGMP Setting > General**.
2. At the IGMP Proxy States, check the checkbox of **Enable**. To enable IP multicast for this WAN Service.

IGMP Setting

General | IGMP Filter | IGMP ACL

The Internet Group Management Protocol (IGMP) is a communication protocol which can be used for more efficient use of online streaming video.

IGMP Proxy State

IGMP Proxy : ☒ Enable ☐ Disable (The settings in this screen are invalid if you select this.)

Query Interval : sec

Query Response Interval : sec

Robustness Value :

IGMP Packet Process

☐ Ignore IGMP packets not from LAN subnet

☐ Ignore IGMP report without router alert option

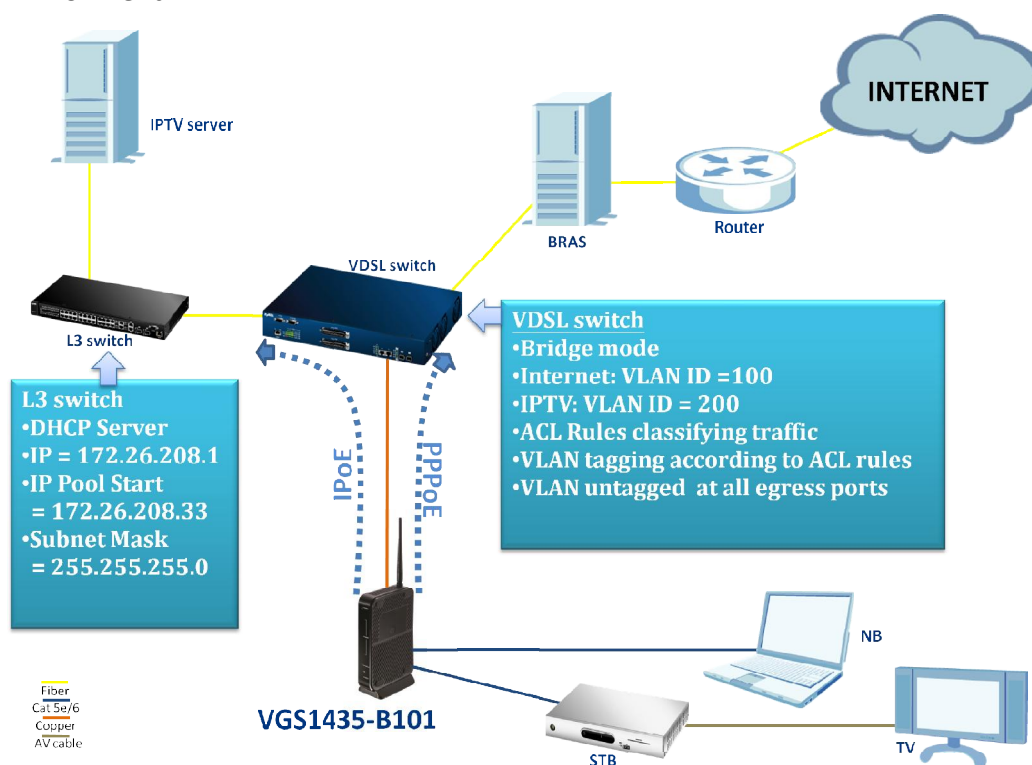
☐ Ignore IGMP leave without router alert option

☐ Ignore IGMP query without router alert option

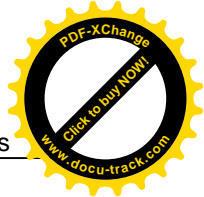
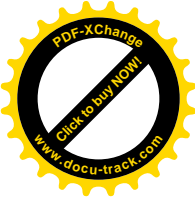
☐ Ignore IGMP query which destination IP is not 224.0.0.1

Protocol Based Scenario

Environment



The Network structure of Central Office depends on the deployment of different ISP (Internet Service Provider) in different environments in different countries. One of the commonly known methods for separating different types of traffic is by classifying their transmitting protocols. In the case of the aforementioned diagram, the INTERNET traffic is encapsulated in the PPoE and the IPTV traffic is encapsulated in the IPoE. The COE (VDSL switch) has the ability to distinguish those 2 traffics and assign the dedicated ACL rules to them. So, how should we configure the VSG1432-B101 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.



WAN Configuration

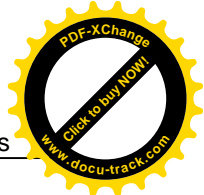
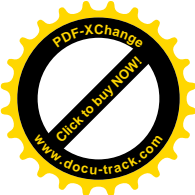
a. INTERNET Service

1. Go to **Network Settings > Broadband**.
2. Click modify icon to modify the WAN service type of VSG1432-B101.
3. Select the WAN service type to be “**PPPoE**”. Also you want to enter the Name.

WAN Configuration

General

Active	<input checked="" type="checkbox"/>
Name:	<input type="text" value="VDSL_test"/>
Type:	<input type="text" value="VDSL"/>
Mode:	<input type="text" value="Routing"/>
Encapsulation:	<input type="text" value="PPPoE"/>



4. Enter the **PPP Username**, e.g. "test@isp.net". Enter the **PPP Password**, e.g. "1234".

PPP Information

PPP User Name :	<input type="text" value="test@isp.net"/>
PPP Password :	<input type="password" value="****"/>
PPP Auto Connect	<input type="checkbox"/>
Idle Timeout [minutes]:	<input type="text" value="5"/>
PPPoE Service Name :	<input type="text"/>
PPPoE Passthrough	<input type="checkbox"/>

5. Click Apply button to save and then review all WAN setup parameters to make sure all related settings are correct; the **IGMP multicast** should be **Disabled**.

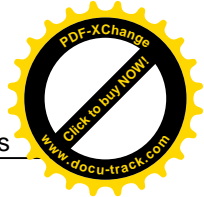
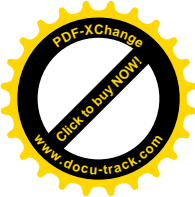
Broadband

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

Add New WAN Interface

#	Status	Name	Type	Encapsulation	VLAN	VP/VC1	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		VDSL_Test	VDSL	PPPoE	N/A	N/A	N/A	N	Y	Y	

Note:
If no default gateway configured, system will select default gateway automatically.



b. IPTV Service

1. Go to **Network Settings > Broadband**.
2. Click **Add New WAN Interface**.

Broadband

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

Add New WAN Interface

#	Status	Name	Type	Encapsulati...	VLAN	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		VDSL_Test	VDSL	PPPoE	N/A	N/A	N/A	N	Y	Y	

Note:
If no default gateway configured, system will select default gateway automatically.

3. Select the Encapsulation type to be **"IPoE"**. Also you want to enter the Name.

WAN Configuration

General

Active: ☒

Name:

Type:

Mode:

Encapsulation:

4. Select **"Obtain an IP address automatically"** in the WAN Configuration Settings page.

IP Address

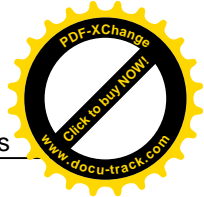
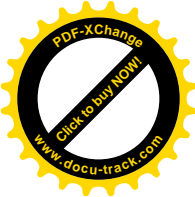
☒ Obtain an IP Address Automatically

☐ Static IP Address

IP Address :

Subnet Mask :

Gateway IP address :



5. We don't enable the NAT at this IPTV WAN service; but we need to check the checkbox for **IGMP Proxy Enable**.

Routing Feature

NAT Enable	<input type="checkbox"/>
IGMP Proxy Enable	<input checked="" type="checkbox"/>
Apply as Default Gateway	<input type="checkbox"/>

6. Click Apply button to save and then review all WAN setup parameters to make sure all related settings are correct.

Broadband

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

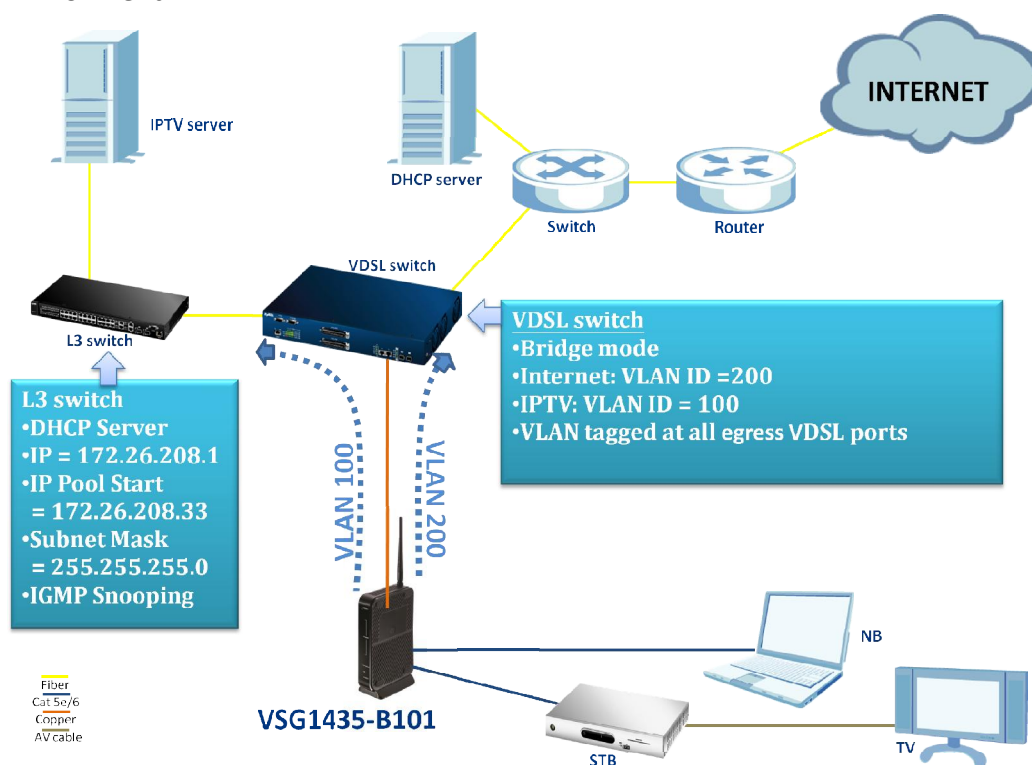
Add New WAN Interface

#	Status	Name	Type	Encapsulati...	VLAN	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		IPTV_test	VDSL	IPoE	N/A	N/A	N/A	Y	N	N	
2		VDSL_Test	VDSL	PPPoE	N/A	N/A	N/A	N	Y	Y	

Note:
If no default gateway configured, system will select default gateway automatically.

VLAN Based Scenario

Environment



The Network structure of Central Office depends on the deployment of different ISP (Internet Service Provider) in different environments in different countries. One of the commonly known methods for separating different types of traffic is by classifying their VLAN ID. In the case of the aforementioned diagram, the INTERNET traffic is tagged with a VID=100 and the IPTV traffic is tagged with a VID=200. The COE (VDSL switch) receives the already VLAN tagged traffic from the CPE, and handles them according to their VID values. So how should we configure the VSG1432-B101 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.

WAN Configuration

a. IPTV Service

1. Go to **Network Settings > Broadband**.
2. Click **Add New WAN Interface**.

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

[Add New WAN Interface](#)

#	Status	Name	Type	Encapsulati...	VLAN	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		VDSL_Test	VDSL	PPPoE	N/A	N/A	N/A	N	Y	Y	

Note:
If no default gateway configured, system will select default gateway automatically.

3. Select the Encapsulation type to be **"IPoE"**. Also you want to enter the Name.

WAN Configuration

General

Active: ☒

Name:

Type:

Mode:

Encapsulation:

4. Select **"Obtain an IP address automatically"** in the WAN Configuration Settings page.

IP Address

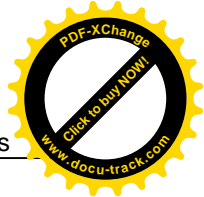
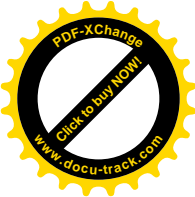
☒ Obtain an IP Address Automatically

☐ Static IP Address

IP Address :

Subnet Mask :

Gateway IP address :



5. We don't enable the NAT at this IPTV WAN service; but we need to check the checkbox for **IGMP Proxy Enable**.

Routing Feature

NAT Enable	<input type="checkbox"/>
IGMP Proxy Enable	<input checked="" type="checkbox"/>
Apply as Default Gateway	<input type="checkbox"/>

6. Enter the **802.1P priority 5** and **802.1Q VLAN ID 100**

VLAN

Active	<input checked="" type="checkbox"/>
802.1p :	<input type="text" value="5"/>
802.1q :	<input type="text" value="100"/> (0~4094)

7. Click Apply button to save and then review all WAN setup parameters to make sure all related settings are correct.

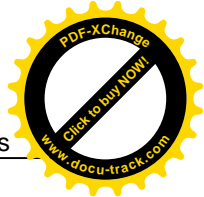
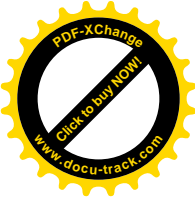
Broadband

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

Add New WAN Interface

#	Status	Name	Type	Encapsulati...	VLAN	VP/VC/CI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		VDSL_Test	VDSL	PPPoE	N/A	N/A	N/A	N	Y	Y	
2		IPTV_test	Ethernet	IPoE	5/100	N/A	N/A	Y	N	N	

Note:
If no default gateway configured, system will select default gateway automatically.

b. INTERNET Service

1. Go to **Network Settings > Broadband > Add New WAN Interface**.
2. Set the WAN Service Configuration to **PPP over Ethernet (PPPoE)**.
3. Check **Active** box of VLAN item and enter **802.1P priority 3** and **802.1Q VLAN ID 200**.

General

Active	<input checked="" type="checkbox"/>
Name:	<input type="text" value="VDSL_Test"/>
Type:	<input type="text" value="VDSL"/>
Mode:	<input type="text" value="Routing"/>
Encapsulation:	<input type="text" value="PPPoE"/>

VLAN

Active	<input checked="" type="checkbox"/>
802.1p :	<input type="text" value="3"/>
802.1q :	<input type="text" value="200"/> (0~4094)

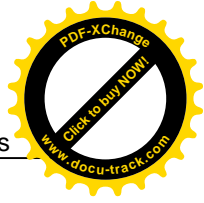
4. Enter the **PPP Username** and **PPP Password**, check **Enable NAT** box and **Apply as Default Gateway** box.

PPP Information

PPP User Name :	<input type="text" value="test"/>
PPP Password :	<input type="password" value="....."/>
PPP Auto Connect	<input type="checkbox"/>
Idle Timeout [minutes]:	<input type="text" value="5"/>
PPPoE Service Name :	<input type="text"/>
PPPoE Passthrough	<input type="checkbox"/>

Routing Feature

NAT Enable	<input checked="" type="checkbox"/>
IGMP Proxy Enable	<input type="checkbox"/>
Apply as Default Gateway	<input checked="" type="checkbox"/>



5. Click Apply button to save and then review all WAN setup parameters to make sure all related settings are correct.

Broadband

Correct Internet connection settings get you online. You might need to consult the Internet Service Provider (ISP) for the following settings.

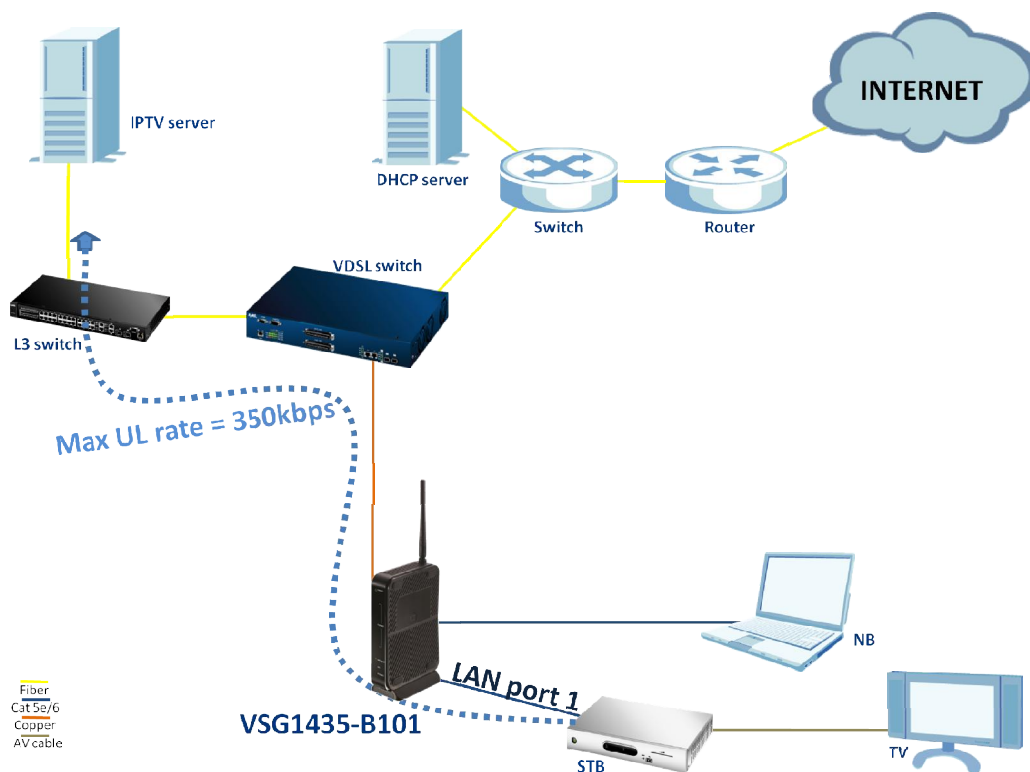
Add New WAN Interface

#	Status	Name	Type	Encapsulati...	VLAN	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		VDSL_test	VDSL	PPPoE	3/200	N/A	N/A	N	Y	Y	
2		IPTV_test	Ethernet	IPoE	5/100	N/A	N/A	Y	N	N	

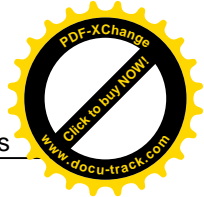
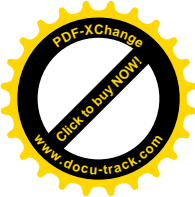
Note:
If no default gateway configured, system will select default gateway automatically.

Quality of Service

Environment



The “Quality of Service” feature in VSG1432-B101 has the ability to assign different task in accordance with the chosen type of traffic. In the case of the aforementioned diagram, we would like to limit the maximum upload rate of the IPTV service to 350 kbps. So how should we configure the VSG1432-B101 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.



QoS configuration

a. Enable QoS

1. Go to **Network Settings > QoS**.
2. Check the **Active QoS** box.

QoS

General Queue Setup Class Setup Policer Setup Monitor

Quality of Service(QoS) defines the traffic priority of Internet services to the home network.

QoS :

State : ☒ Enable ☐ Disable (The settings of Qos are invalid if you select this.)

3. Go to **Network Settings > QoS > Queue Setup**.
4. Click **Add New Queue**.

QoS

General Queue Setup Class Setup Policer Setup Monitor

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

Queue Setup

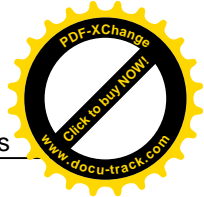
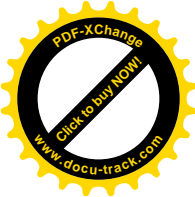
Add new Queue

Current Settings :

Queue

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
---	--------	------	-----------	----------	--------	-------------------	-------------------	--------

Note:
Maximum of 8 configurable entries for WAN port, and maximum of 3 configurable entries for LAN port.
If queue is deleted, then related classifiers will be removed too.
Priority level "1" is the highest priority for QoS.

**b. Configure the Video traffic.**

1. Check the **Enable** box.
2. Enter the **Queue Name** box, e.g. "Queue1".
3. Select the **Outgoing interface**, e.g. "WAN".
4. Select the **Priority** as "2".
5. Select the **Weight** as "3".
6. Click **Apply**.

QoS Queue Configuration

Queue Settings

☒ Active

Name : Queue1

To Interface : WAN

Priority : 2

Weight : 3

Buffer Management : Drop Tail (DT)

Rate Limit : 0 (kpbs)

Apply Cancel

7. Go to **Network Settings > QoS > Class Setup**.
8. Click **Add New Classifier**.

QoS

General Queue Setup **Class Setup** Policer Setup Monitor

A classifier groups traffic into data flows according to specific criteria. Class Setup can add, edit, or delete QoS classifiers.

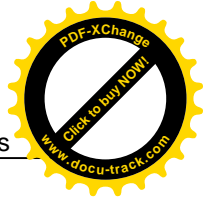
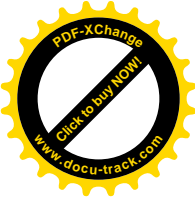
Class Setup

Add new Classifier

Current Settings :

▪ Class

#	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
---	--------	------------	-------------------------	-----------	-------------	-------------	----------	--------



9. Check the **Enable** box.
10. Enter the **Name**, e.g. "Video".
11. Select the **Classification Order** to be "Last".
12. Select the **Ether Type** to be "IP (0x800)".
13. Check the **From Interface** to be "LAN1".
14. Click **Apply**.

Please fill up steps 1 through 4 to configure a QoS rule.

Step1: Class Configuration

☒ Active

Class Name :

Classification Order :

Step2: Criteria configuration

Use the fields below to specify the characteristics of a data flow that needs to be managed by this QoS rule

Basic

From Interface :

To Interface :

Ether Type :

Source

<input type="checkbox"/> Address	<input type="text"/>	Subnet Netmask	<input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input type="text"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input type="text"/>	MAC Mask	<input type="text"/>	<input type="checkbox"/> Exclude

Destination

<input type="checkbox"/> Address	<input type="text"/>	Subnet Netmask	<input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input type="text"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input type="text"/>	MAC Mask	<input type="text"/>	<input type="checkbox"/> Exclude

Others

<input type="checkbox"/> Service	<input type="text" value="Age of Empires"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> IP protocol	<input type="text" value="TCP"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> DHCP	<input type="text" value="Vendor Class ID (DHCP Option 60)"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Packet Length	<input type="text"/> ~ <input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> DSCP	<input type="text" value="0"/> (0~63)	<input type="checkbox"/> Exclude
<input type="checkbox"/> 802.1P	<input type="text" value="0 BE"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> VLAN ID	<input type="text"/> (1~4094)	<input type="checkbox"/> Exclude
<input type="checkbox"/> TCP ACK		<input type="checkbox"/> Exclude

Step3: Packet modification

The content of the packet can be modified by applying the following settings:

DSCP Mark : (0~63)

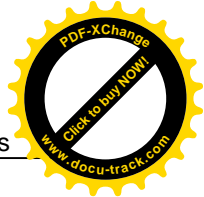
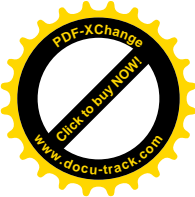
802.1P Mark :

VLAN ID : (1~4094)

Step4: Outgoing queue selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface. Choose "Q_DROP" if you want to drop this kind of traffic.

To Queue Index :



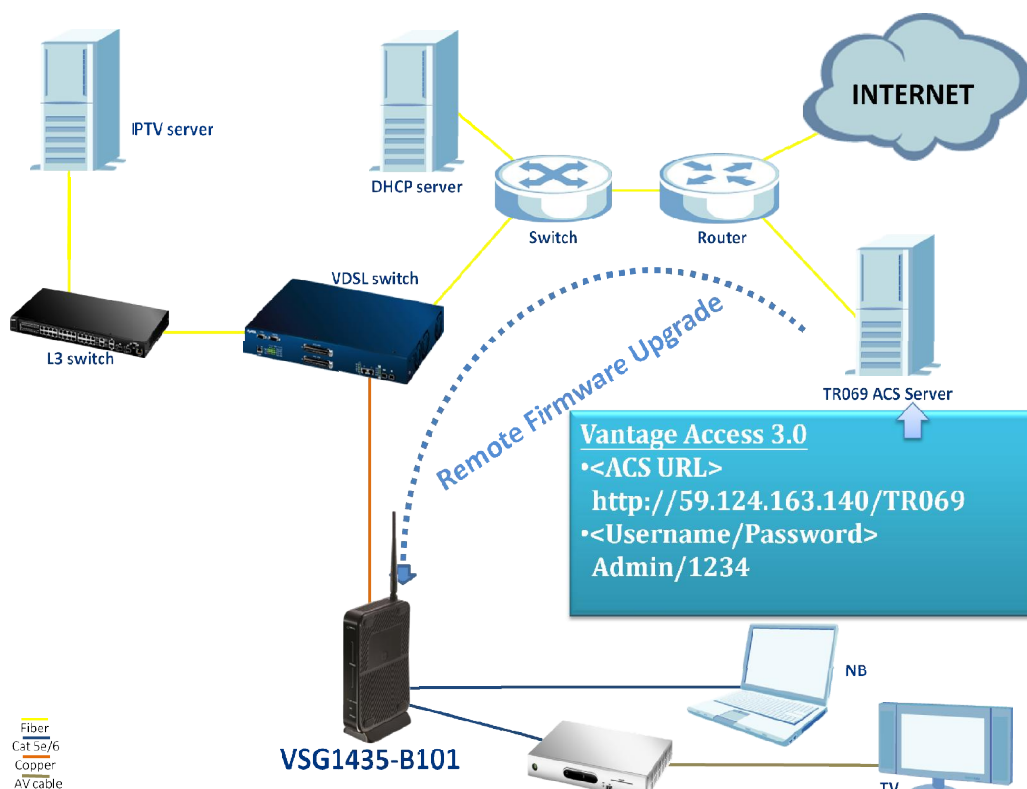
c. Configure the Video traffic Policer.

1. Go to **Network Settings > QoS > Policer Setup** Setup
2. Click **Add New Policer**.

3. Check the **Enable** box.
4. Enter the **Policer Name** box, e.g. "test".
5. Select the **Meter Type** as "Simple Token Bucket".
6. Enter the **Committed Rate** as "350".
7. Enter the **Committed Burst Size** as "100".
8. Select the Class in **Available Class field** and add to **Selected Class**.

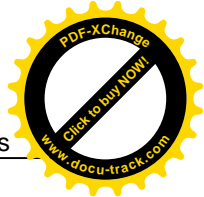
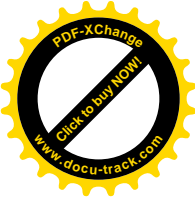
TR069 – Remote Firmware Upgrade

Environment



The VSG1432-B101 provides the TR-069 remote management feature; it could speed up the deployment of CPEs and ease our supporting costs. It can also help the VDSL ISP (Internet Service Provider) to reduce operation effort as well as enhance customer satisfaction. In the case of the aforementioned diagram, the TR069 ACS server remote upgrades the firmware of CPE. So how should we configure the VSG1432-B101 to fit the aforementioned scenario? The following step-by-step procedure instructs us the method.

Note: This document uses a ZyXEL ACS server, Vantage Access 3.0, as a reference.



TR069 Configuration

a. Check the current firmware version.

1. Click **Status**.

The screenshot shows the 'Status' page of a ZyXEL device. It contains a table with the following information:

Device Information	
Host Name:	ZyXEL
Model Number:	VSG1435-B101
Firmware Version:	1.10(TUB.0)b6

As we can see, the Firmware Version is 1.10(TUB.0)b6.

b. Configure the required TR069 parameters for the ACS server.

1. Go to **Maintenance > Remote Management > TR069 Client**.
2. Check the **Enable** box.
3. Enter the **Inform Interval**, e.g. "30" seconds.
4. Enter the **ACS URL**, e.g. "<http://59.124.163.140/TR069>".
5. Enter the **ACS User Name**, e.g. "admin".
6. Enter the **ACS Password**, e.g. "1234".
7. Select the **WAN Interface used by TR-069 client**, e.g. "Any_WAN".
8. Click **Apply**.

The screenshot shows the 'Remote Management' page with the 'TR-069 Client' tab selected. It includes a description of TR-069 and configuration fields:

TR-069 is a remote management tool on your device. The operator can upgrade firmware, modify settings, and diagnose problems remotely when you enable TR-069.

Inform: ☒ Enable ☐ Disable

Inform Interval:

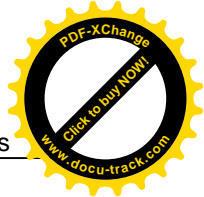
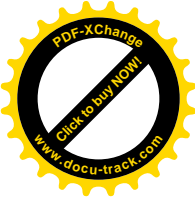
ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console: ☐ Enable ☒ Disable

**ACS server (Vantage Access 3.0)**

Make sure that the VSG1432-B101 is correctly subscribed on the ACS server.

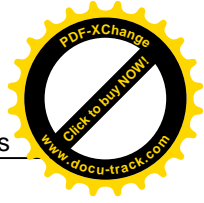
DeviceName :ZyXEL
OUI-SN :404A03-404A0367E018

Device List

Device List							
Index	Device Name	MAC	Device Type	Software Version	Status	CPE/IGD	Owner
1	ZyXEL	404A03-404A0367E018	VSG1435-B101	1.10(TUB.0)b6	Off	Gateway	test

1/1

As we can see, a VSG1432-B101 is subscribed on the server and the SW Version is 1.10(TUB.0)b6.



NAT Port Forwarding

NAT/Multi-NAT Introduction

- What is Multi-NAT?

The 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, one 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 the IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

- How NAT works?

If we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA), see the following figure. 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.

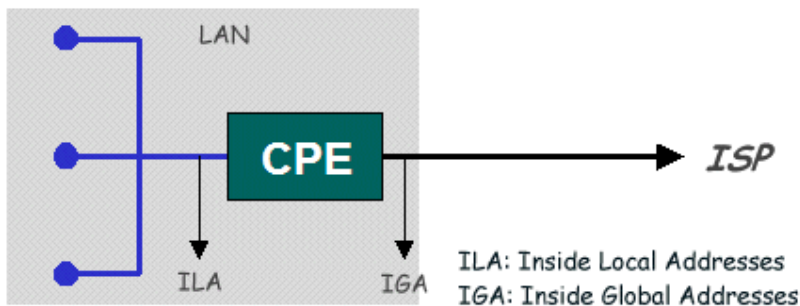


Figure1: Local/Global IP Addresses

- NAT Mapping Types

The NAT supports five types of IP/port mapping. They are:

1. **One to One**

In One-to-One mode, the Prestige maps one ILA to one IGA.

2. **Many to One**

In Many-to-One mode, the CPE maps multiple ILAs to one IGA.

3. **Many to Many Overload**

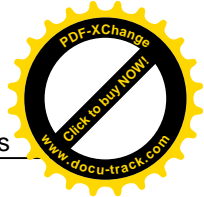
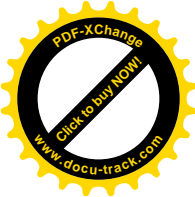
In Many-to-Many Overload mode, the CPE maps the multiple ILAs to shared IGA.

4. **Many to Many No Overload**

In Many-to-Many No overload mode, the CPE maps each ILA to unique IGA.

- Server (DMZ host)

In Server mode (DMZ host), the CPE maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note: If you want to map each server to one unique IGA, please use the One-to-One mode.



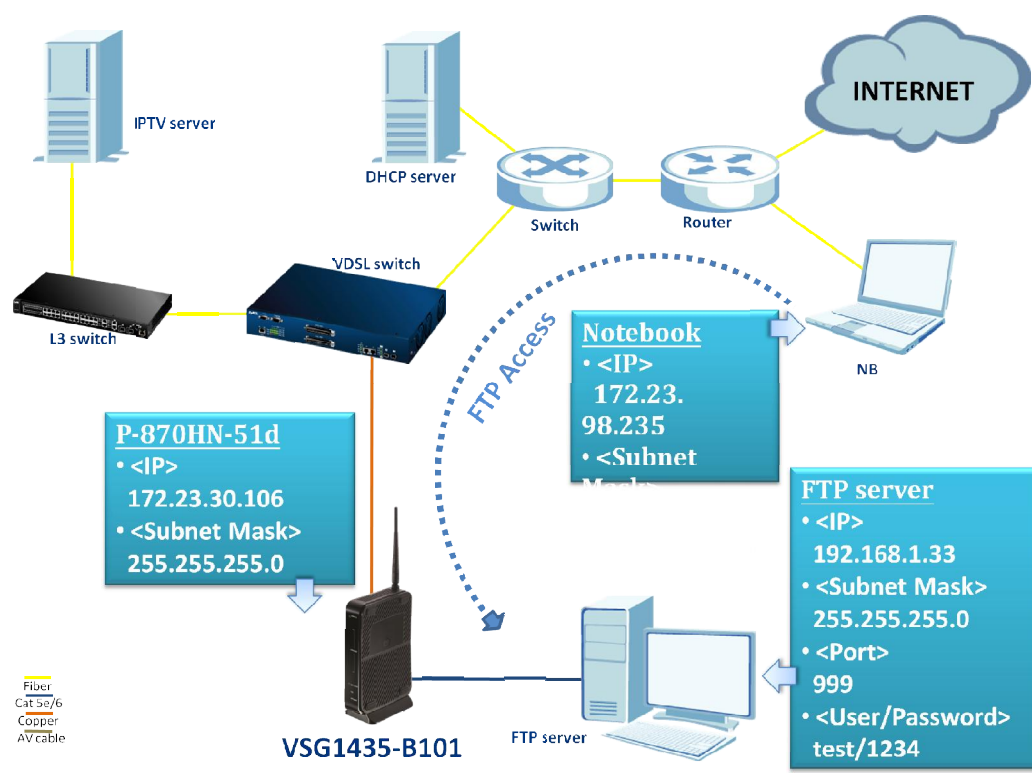
The following table summarizes these types.

NAT Type	IP Mapping	Mapping Direction
One-to-One	ILA1<--->IGA1	Both
Many-to-One	ILA1---->IGA1 ILA2---->IGA1 ...	Outgoing
Many-to-Many Overload	ILA1---->IGA1 ILA2---->IGA2 ILA3---->IGA1 ILA4---->IGA2 ...	Outgoing
Many-to-Many Overload (Allocate Connections)	No ILA1---->IGA1 ILA2---->IGA3 ILA3---->IGA2 ILA4---->IGA4 ...	Outgoing
Server	Server 1 IP<----IGA1 Server 2 IP<----IGA1	Incoming

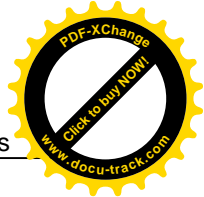
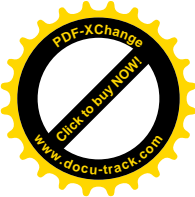
- Port numbers for some services:

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

Environment



The NAT provides system administrators an easy solution to create a private IP network for security and IP management. Powered by NAT technology, the VSG1432-B101 supports complete the NAT mapping and most popular Internet multimedia applications. This feature is the best described with the NAT port forwarding feature implemented in the CPE. In the case of the above diagram, we have a FTP server installed behind the CPE with an IP assigned by the local DHCP server (192.168.1.33). How should we configure the VSG1432-B101, so that the notebook at the WAN site can access the FTP server? The following step-by-step procedure instructs us the method.



Port Forwarding Configuration

a. Show the device information.

1. Click **Status**.

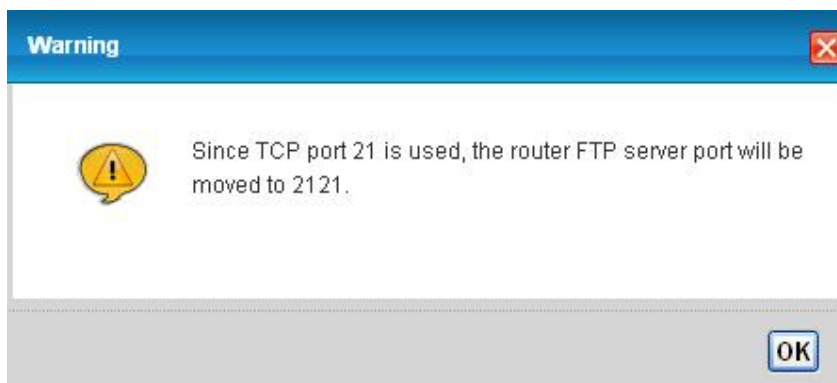
Status	
Device Information	
Host Name:	ZyXEL
Model Number:	VSG1435-B101
Firmware Version:	1.10(TUB.0)b6
WAN Information:	
- WAN Type:	VDSL
- MAC Address:	02:10:18:01:00:04
- IP Address:	61.216.176.185
- Encapsulation:	PPPoE

We can see that the WAN is assigned with IP = 61.216.176.185

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

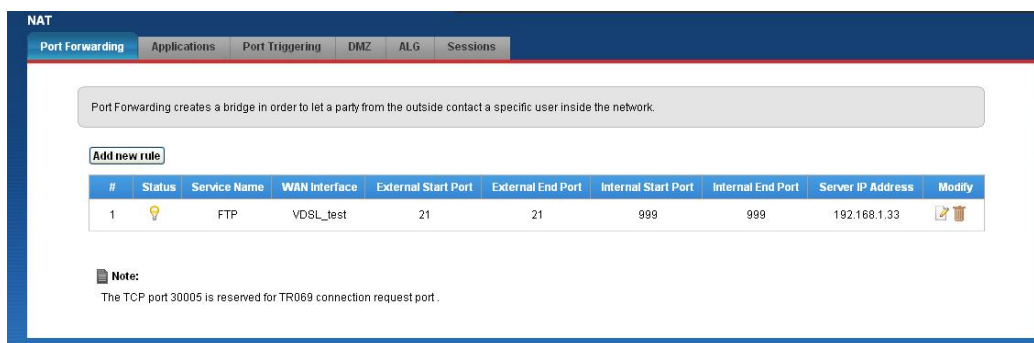
1. Go to **Network Settings> NAT > Port Forwarding**.
2. Select the **Service Name**, e.g. "FTP".
3. Select the **WAN Interface**, e.g. "VDSL_test".
4. Enter the **Server IP Address**, e.g. "192.168.100.33".
5. Enter the **External port Start**, e.g. "21".
6. Enter the **External port End**, e.g. "21".
7. Enter the **Internal port Start**, e.g. "999".
8. Enter the **Internal port End**, e.g. "999".
9. Select the **Protocol**, e.g. "TCP".
10. Click **Apply**.

A warning message as followed will pop up:

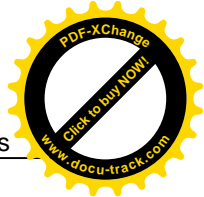
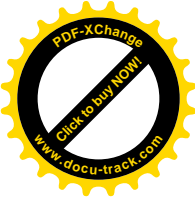


This phenomenon is normal, because the CPE itself can be accessed by the FTP, which the port is also 21. Since we are creating a new rule using port 21, the default port number of the CPE's FTP server port will automatically be moved to 2121.

A new port forwarding rule is now created.



Show the IP configuration of notebook:



```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

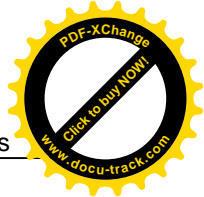
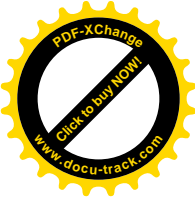
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : zyxel.com.tw
    IP Address. . . . . : 172.23.98.235
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 172.23.97.1
```

Use the notebook to access the FTP server with IP = 61.216.176.185

```
C:\Users\Ansa>ftp 61.216.176.185
已連線到 61.216.176.185。
220----- Welcome to Pure-FTPd [TLS] -----
220-You are user number 1 of 10 allowed.
220-Local time is now 02:31. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
使用者 (61.216.176.185:(none)): admin
331 User admin OK. Password required
密碼:
230 OK. Current restricted directory is /
ftp>
```



DMZ Host Configuration

If we enable the DMZ host, it will open up all the internal ports to the dedicated Server IP (in this case, IP = 192.168.100.35) allowing client at the WAN side to access the FTP server via port forwarding.

a. Create a DMZ host.

1. Go to **Network Settings > NAT > DMZ**.
2. Enter the IP of the **Default Server Address**, e.g. "192.168.100.35".
3. Click **Apply**.

NAT

Port Forwarding Applications Port Triggering **DMZ** ALG Sessions

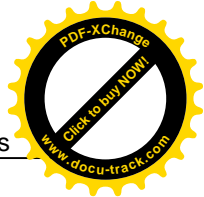
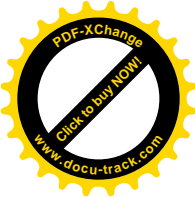
The Demilitarized Zone (DMZ) allows the computers connected to the device to be exposed to the Internet.

Default Server Address :

Note:
Enter IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.

Use the notebook to access the FTP server with IP = 61.216.176.185

```
C:\Users\Ansa>ftp 61.216.176.185
已連線到 61.216.176.185。
220----- Welcome to Pure-FTPd [TLS] -----
220-You are user number 1 of 10 allowed.
220-Local time is now 02:31. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
使用者 (61.216.176.185:(none)): admin
331 User admin OK. Password required
密碼:
230 OK. Current restricted directory is /
ftp>
```

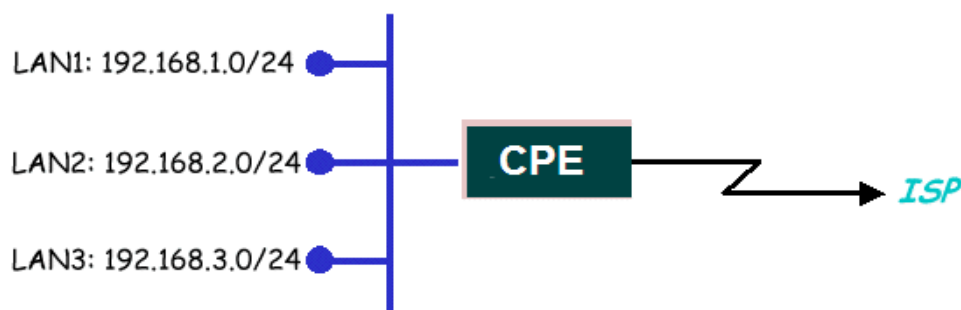



LAN Connection

IP Alias Introduction

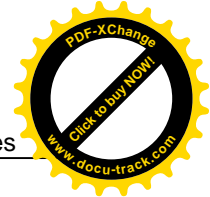
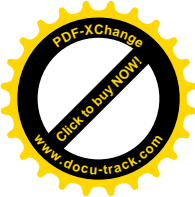
- What is the IP Alias?

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



IP Alias connects three local networks to the Internet

The CPE supports three virtual LAN interfaces via its single physical Ethernet interface. As to the second and third networks, we call '**IP Alias 1**' and '**IP Alias 2**'.



IP Alias Configuration

a. IP Alias

1. Go to **Network > LAN**.
2. Check the **Active IP Alias** box.
3. Enter the **IP Address**, e.g. "10.0.0.1".
4. Enter the **IP Subnet Mask**, e.g. "255.255.255.0".
5. Click **Apply**.

IP Alias

☒ Enable IP Alias

IP Address: 10.0.0.1

IP Subnet Mask: 255.255.255.0

Apply

Client List Configuration

We can manually assign a particular IP to a DHCP client with the specific MAC address.

a. Enable the DHCP server.

1. Go to **Network Settings > Home Networking > LAN Setup**.
2. Enter the **IP Address**, e.g. "192.168.100.1".
3. Enter the **IP Subnet Mask**, e.g. "255.255.255.0".
4. Check the **Enable** box of DHCP Server State.
5. Enter the **Beginning IP Address**, e.g. "192.168.100.33".
6. Enter the **Ending IP Address**, e.g. "192.168.100.254".

Home Networking

LAN Setup Static DHCP UPnP

This page lets you configure the LAN TCP/IP settings and have the VSG1435-B101 as a DHCP server or DHCP relay agent.

Interface Group

Group Name: Default

LAN IP Setup

IP Address: 192.168.100.1

Subnet Mask: 255.255.255.0

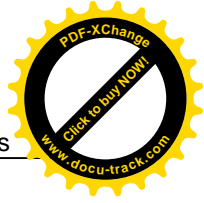
DHCP Server State

DHCP: ☒ Enable ☐ Disable ☐ DHCP Relay

IP Addressing Values

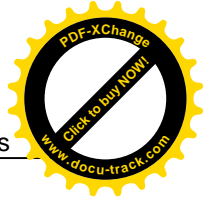
Beginning IP Address: 192.168.100.33

Ending IP Address: 192.168.100.254



- b. Show information on the DHCP server.
1. Login the device by Telnet.
 2. Type the command "lan config" to enter configuration mode.
 3. Type the command "dhcpserver show"

```
> dhcpserver show
dhcpserver: enable
start ip address: 192.168.100.33
end ip address: 192.168.100.64
leased time: 24 hours
```



Using Universal Plug n Play (UPnP)

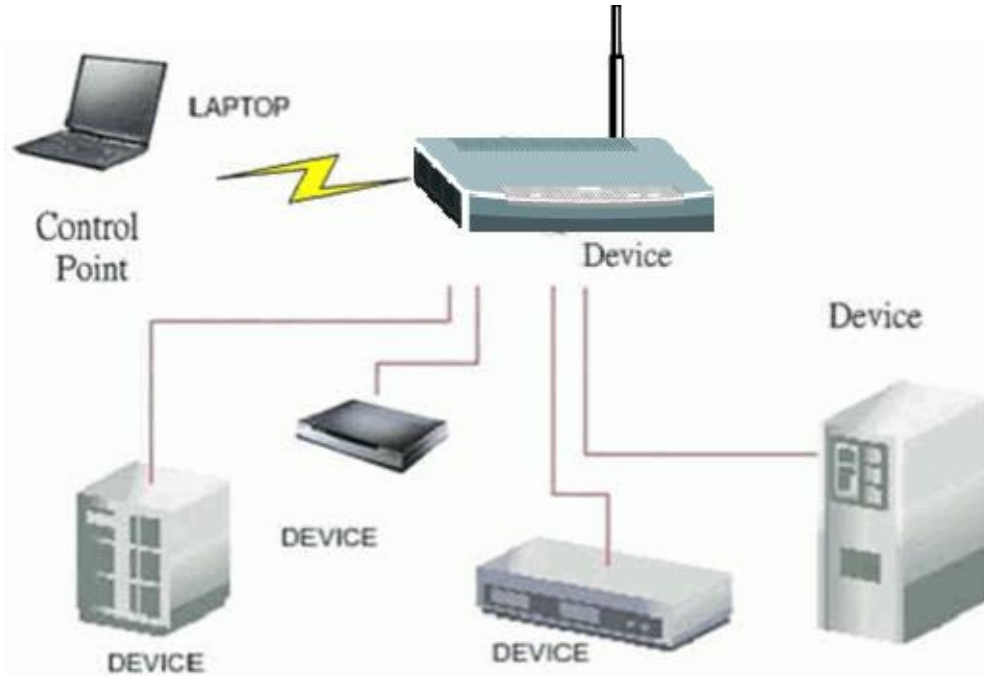
- **1. What is the UPnP?**

The UPnP (Universal Plug and Play) makes the 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 the TCP/IP and Web technologies. The UPnP can be supported essentially in any operating system and works essentially with any type of physical networking media, wired or wireless.

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

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

- **Devices:** Network devices, such as networking gateways, TV, refrigerators, printers, etc, which provide services.
- **Services:** Services are provided by devices, such as time services provided by alarm clocks. In the UPnP, services are described in XML format. Control points can set/get services information from devices.
- **Control points:** Control points can manipulate the 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 the UPnP-enabled devices. These devices respond with their URLs and device descriptions.



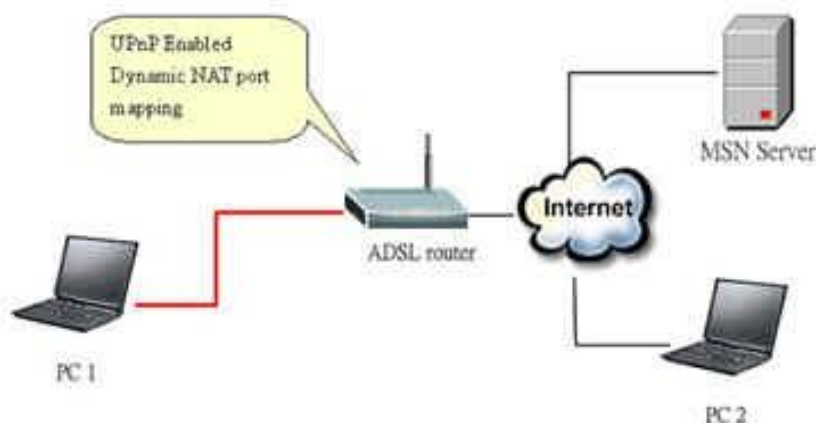
UPnP Operations

- **Addressing:** The UPnP v1 devices MAY support IPv4, IPv6, or both. For IPv4, each device should have the 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 the 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 into the network, it will advertise its 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 the 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 its own control interface by the URL link. So that users can go to the device's presentation Web page by the URL to control this device.

- 2. Using the UPnP in ZyXEL devices.

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

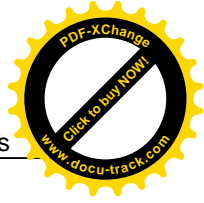
In the diagram, supposing that PC1 and PC2 both sign in MSN server, they would like to establish a video conference. The PC1 is behind the PPPoE dial-up router which supports the UPnP. Since the router supports the UPnP, we don't need to setup the NAT mapping for PC1. As long as we enable the UPnP function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



Device: Device Router

Service: NAT function provided by device Router

Control Point: PC1



Universal Plug n Play (UPnP) Configuration

- a. Activate the UPnP feature.
1. Go to **Network Settings > Home Networking > UPnP**.
 2. Check the **Enable** box.
 3. Click **Apply**.

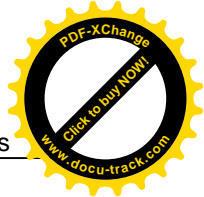
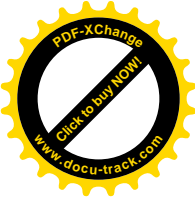
Home Networking

LAN Setup Static DHCP **UPnP**

Universal Plug and Play (UPnP) is a networking standard for easy network connectivity among devices.

State: ☒ Enable ☐ Disable

Apply Cancel



Maintenance Log

Internal Maintenance

The VSG1432-B101 has the ability to record the events happening in the CPE into a system log (according to the severity) and maintain this log in itself.

a. Activate the Maintenance Log.

1. Go to **Maintenance > Logs > Log Settings**.
2. Check the **Enable** box.
3. Select the **Mode**, e.g. "Local File".
4. Click **Apply**.

Logs Setting

Logs Setting defines the level of logs to be recorded and where to send the log history. If the log mode is enabled, the system will begin to record selected logs.

Syslog Logging

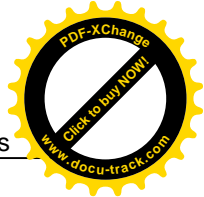
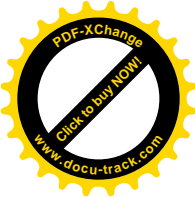
☒ Active

Mode:

Local File

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

UDP Port :



b. Show the log in the Web GUI.

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

Log

System Log Security Log

System Log records the events that occurred on the device. You can check the status of events or send the information to an email account.

Level: Category:

#	Time	Facility	Level	Messages
1	1970 Jan 7 05:07:18	System	info	br0: port 6(eth10.1) entering disabled state
2	1970 Jan 7 05:07:18	System	info	device eth10 left promiscuous mode
3	1970 Jan 7 05:07:18	System	info	device eth10.1 left promiscuous mode
4	1970 Jan 7 05:07:18	System	crit	eth10 Link DOWN.
5	1970 Jan 7 05:07:18	System	info	device ptm0 entered promiscuous mode
6	1970 Jan 7 05:07:18	System	info	BCMVLAN : ptm0 mode was set to RG
7	1970 Jan 7 05:07:18	System	info	ptm0.1 MAC address set to 02:10:18:01:00:04
8	1970 Jan 7 05:07:18	System	info	bcmotmfcfg: Connection UP, LinkActiveStatus=0x1, US=38037000, DS=94681000
9	1970 Jan 7 05:07:18	System	info	XTM Init: 400 tx BDs at 0xa2ac2000
10	1970 Jan 7 05:07:18	System	info	[DoCreateDeviceReq 2449]: register_netdev done

c. Show the log by Telnet.

1. Login the device by Telnet,
2. Type the command "syslog dump".

```
Usage: syslog dump
       syslog help
> syslog dump
===== Dump of Syslog =====
Jan  1 01:12:32 | syslog.emerg BCM96345 started: BusyBox v1.00 (2010.08.11-09:55+0000)
```

Remote Maintenance

The VSG1432-B101 also has the ability to send the system log outside the CPE. Let's say that we want the system log to be sent to the notebook with IP = 192.168.1.101.

a. Activate the Maintenance Log.

1. Go to **Maintenance > Log Settings**.
2. Check the **Active** box.
3. Select the **Mode**, e.g. "Remote"
4. Enter the **Syslog Server IP Address** to be "192.168.100.101".
5. Click **Apply**.

Syslog Logging

☒ Active

Mode:

Remote

Syslog Server IP Address :

192.168.100.101

(Server NAME or IP Address)

UDP Port :

514

We can see the system logs being sent from the CPE by opening Ethereal in the notebook.

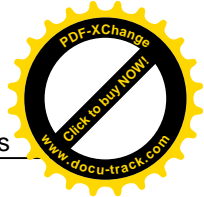
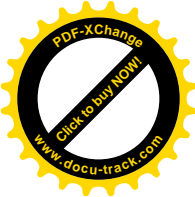
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) : Capturing - Wireshark

Filter: `!(ip.dst == 192.168.1.1) && syslog`

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.1.101	Syslog	SYSLOG.EMERG: BCM96345 started: BusyBox v1.00 (2009.01.06-12:09+0000)
3	0.652418	192.168.1.1	192.168.1.101	Syslog	USER.NOTICE: kernel: klogd started: BusyBox v1.00 (2009.01.06-12:09+0000)
14	25.898291	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: device w10 entered promiscuous mode
16	25.965802	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: port 5(w10) entering learning
18	25.966185	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: topology change detected, port 5(w10) entering forwarding
20	25.966504	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: port 5(w10) entering forwarding
26	29.351121	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: port 5(w10) entering learning
28	30.427353	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: port 5(w10) entering learning
30	30.427872	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: topology change detected, port 5(w10) entering forwarding
32	30.428330	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: port 5(w10) entering forwarding
37	31.288907	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: device w10 left promiscuous mode
39	31.289264	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: br0: port 5(w10) entering learning
42	31.522558	192.168.1.1	192.168.1.101	Syslog	USER.INFO: kernel: device w10 entered promiscuous mode

Frame 1 (103 bytes on wire, 103 bytes captured)

- Ethernet II, Src: ZyxelCom_00:00:01 (00:19:cb:00:00:01), Dst: ZyxelCom_65:87:41 (00:13:49:65:87:41)
- Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.101 (192.168.1.101)
- User Datagram Protocol, Src Port: 32769 (32769), Dst Port: syslog (514)
- Syslog message: SYSLOG.EMERG: BCM96345 started: BusyBox v1.00 (2009.01.06-12:09+0000)
 - 0010 1... = Facility: SYSLOG - messages generated internally by syslogd (5)
 - 0000 = Level: EMERG - system is unusable (0)
 - Message: BCM96345 started: BusyBox v1.00 (2009.01.06-12:09+0000)



Maintenance Tool

Maintenance Procedure

a. Upload Firmware.

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

Firmware Upgrade

Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You may download the latest firmware from the official website.

Current Firmware Version: 1.10(TUB.0)b6

File Path: 102BLLOC0_0818.bin

2. Click **Browse.**
3. Select the Firmware to upload and click Open.
4. Click **Upload.**

b. Save Configuration.

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

Configuration

In Configuration you can save the current device settings in a backup file in your computer, or recover the system by restoring the backup file. You can also reset the device back to factory default.

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

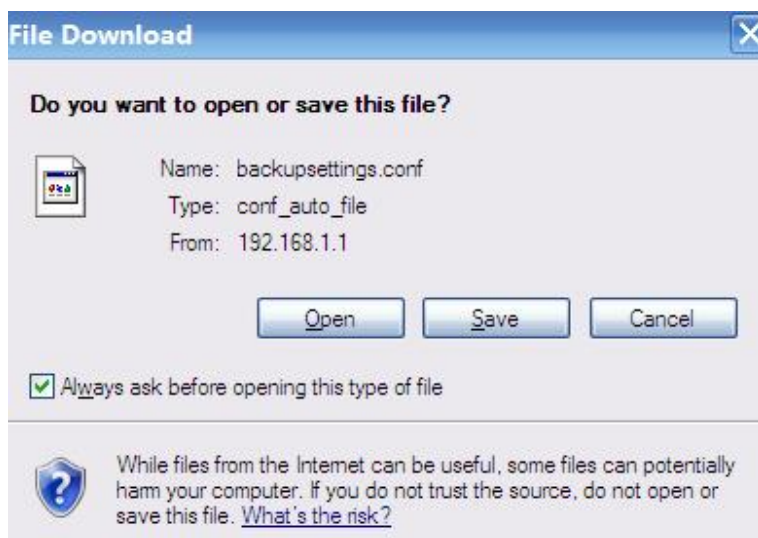
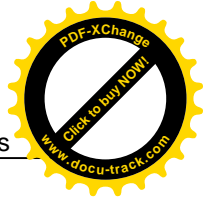
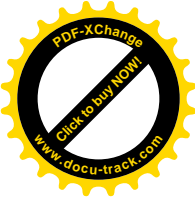
File Path: 未選擇檔案

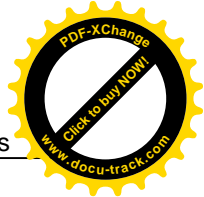
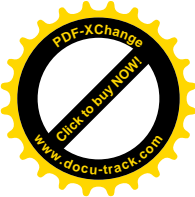
Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

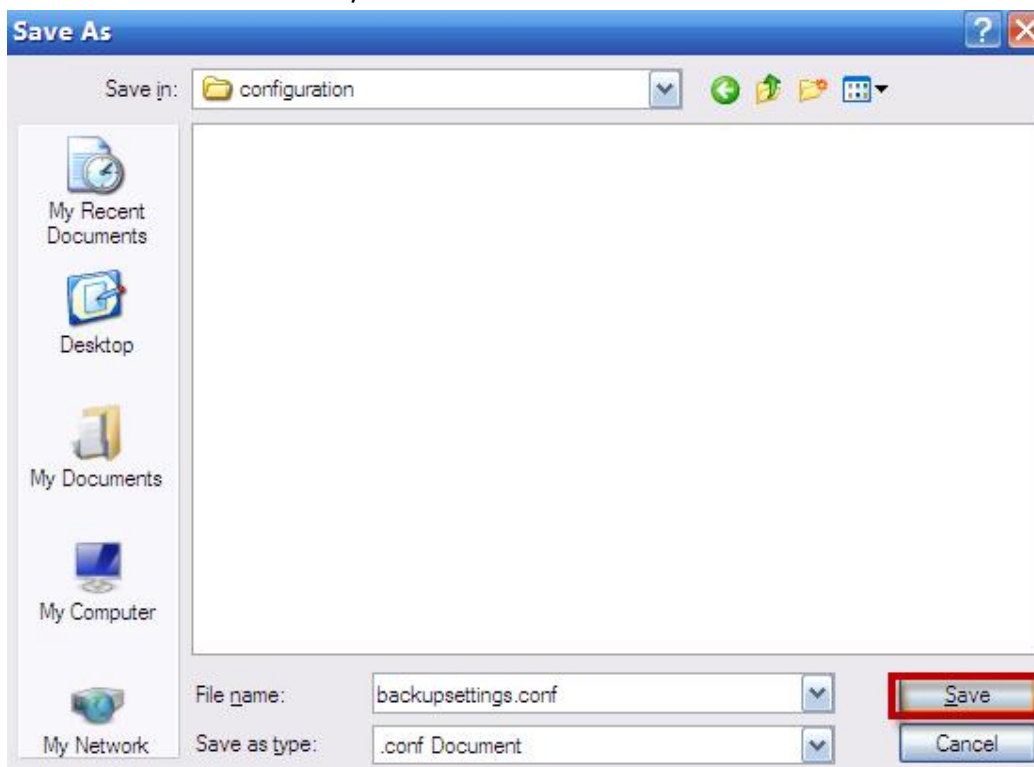
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

2. Click **Backup.**
3. Click **Save.**





4. Select the directory to save and click Save.



c. Upload Configuration.

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

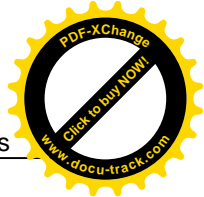
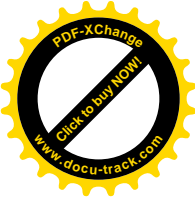
Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path :

2. Click **Browse.**
3. Select the configuration file to upload and click Open.





Wireless Application Notes

Wireless Introduction

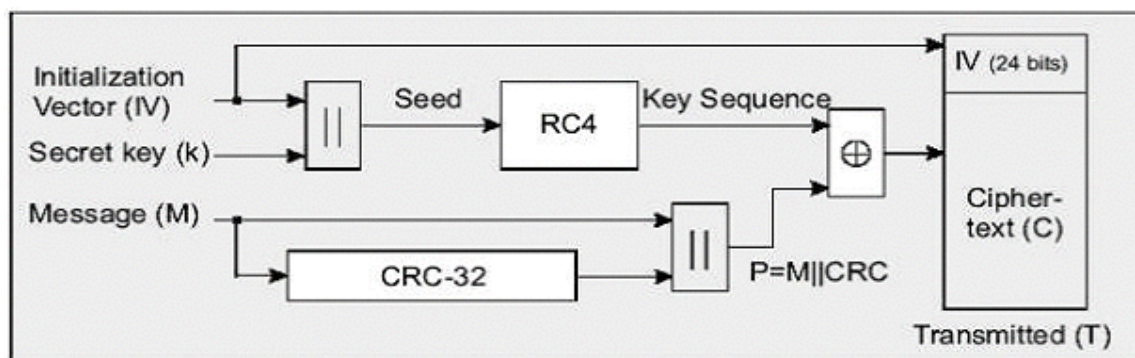
WEP Configuration (Wired Equivalent Privacy) Introduction

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

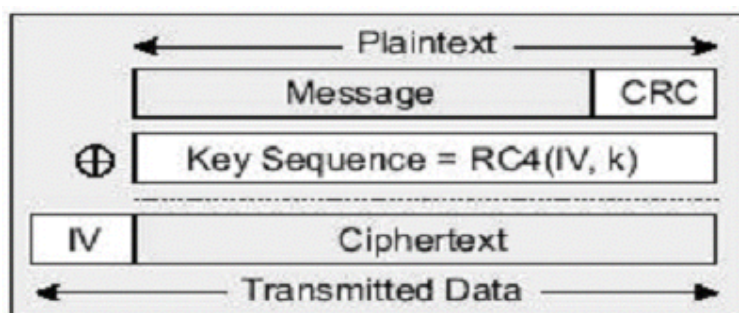
The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping, because the wireless transmissions are easier to intercept than transmissions over wired networks, and wireless is a shared medium. Everything that is transmitted or received over a wireless network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



The 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. The WEP keys (secret key) are 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.



Setting up the Access Point



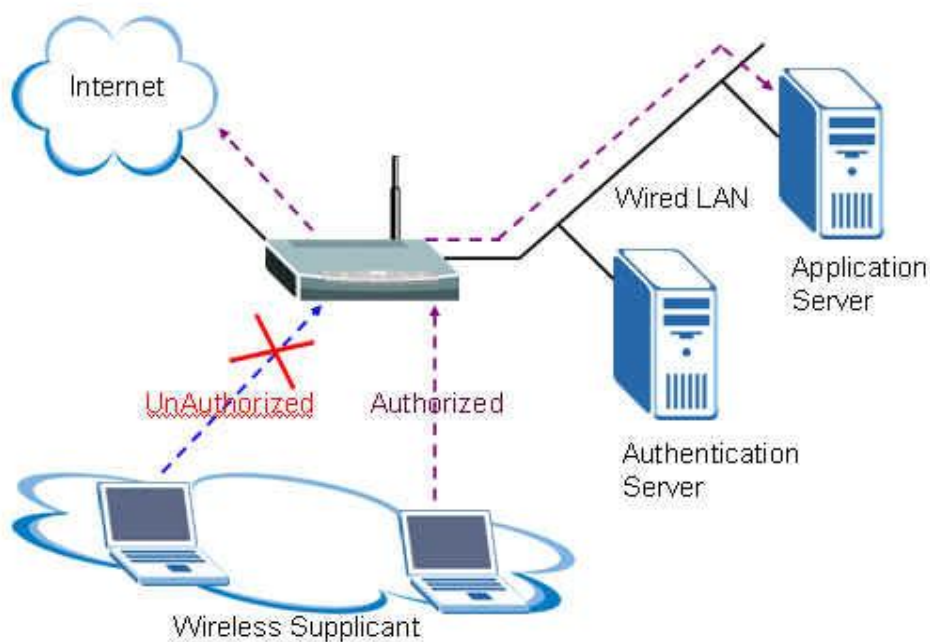
Most access points and clients have the ability to hold up to the 4 WEP keys simultaneously. You need to specify one of the 4 keys as default Key for data

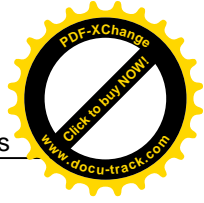
encryption. To set up the Access Point, you will need to set one of the following parameters:

- 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 desired to prevent the unauthorized devices (clients) from gaining access to the network. As the LANs extend to hotels, airports and corporate lobbies, the 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 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 case of the failure of authentication process.





The IEEE 802.1x authentication is a client-server architecture delivered with the 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 accessing any services offered by the Wireless AP. The 802.1x contains three major components:

1. Authenticator:

The device (i.e. Wireless AP) facilitates the authentication for supplicant (Wireless client) attached on the Wireless network. Authenticator controls the physical access to the network based on the authentication status of 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 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 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 client. It validates the identity of the supplicant. Because the authenticator acts as the proxy, the authentication service is transparent to the supplicant.

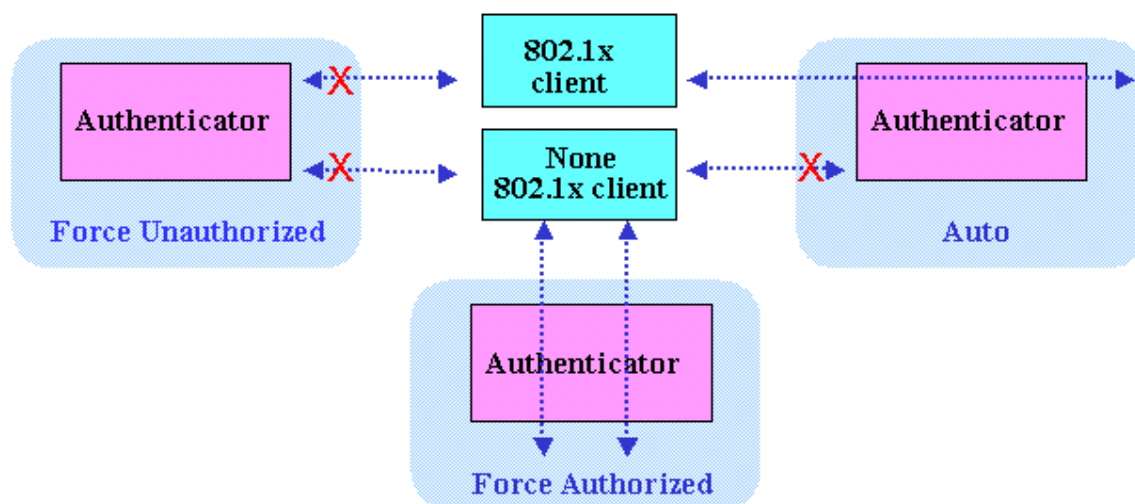
Some Wireless AP (i.e. ZyXEL Wireless AP) have built-in authentication server, therefore the external RADIUS authentication server is not needed. In this case, the Wireless AP is acted as both authenticator and authentication server.

- ***Authentication Port State and Authentication Control***

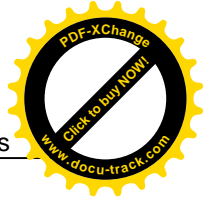
The port state determines whether or not the supplicant (Wireless Client) is granted access to the network behind Wireless AP. There are two authentication port state on the AP, **authorized state** and **unauthorized state**.

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



1. Force Authorized: Disables the 802.1x and causes the port to transit to the authorized state without any authentication exchange required. The port transmits and receives the normal traffic without the 802.1x-based authentication of client. This is the default port control setting. While the AP is setup 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 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 the 802.1x 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 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 the AP is setup as **Auto**, only the Wireless client supporting the 802.1x client can access the network.

- ***Re-Authentication***

The administrator can enable the 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 to reinitiate authentication process. In the ZyXEL Wireless AP 802.1x implementation, if you do not specify a time period before enabling the re-authentication, the number of seconds between re-authentication attempts is 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 the 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.

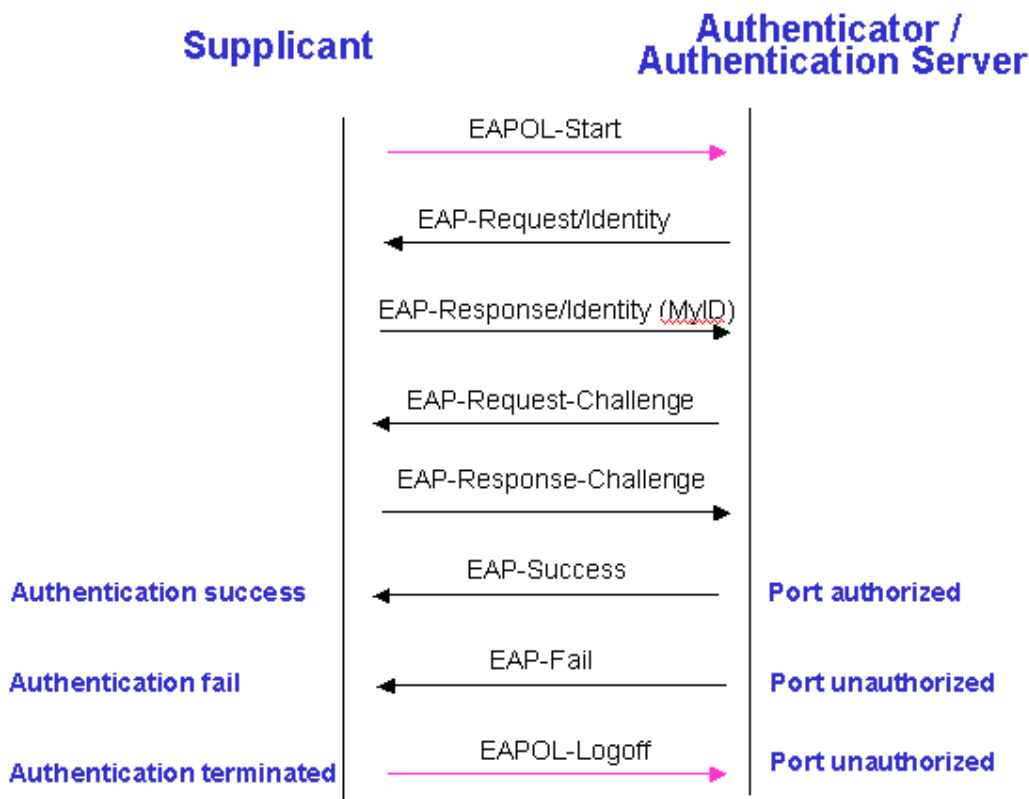
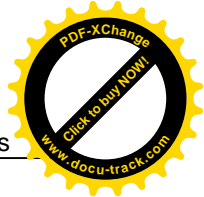
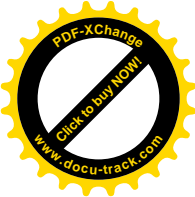


The EAP protocol can support multiple authentication mechanisms, such as MD5-challenge, One-Time Passwords, Generic Token Card, TLS and TTLS etc. Typically, the authenticator will send an initial Identity Request followed by one or more Requests for authentication information. When supplicant receives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

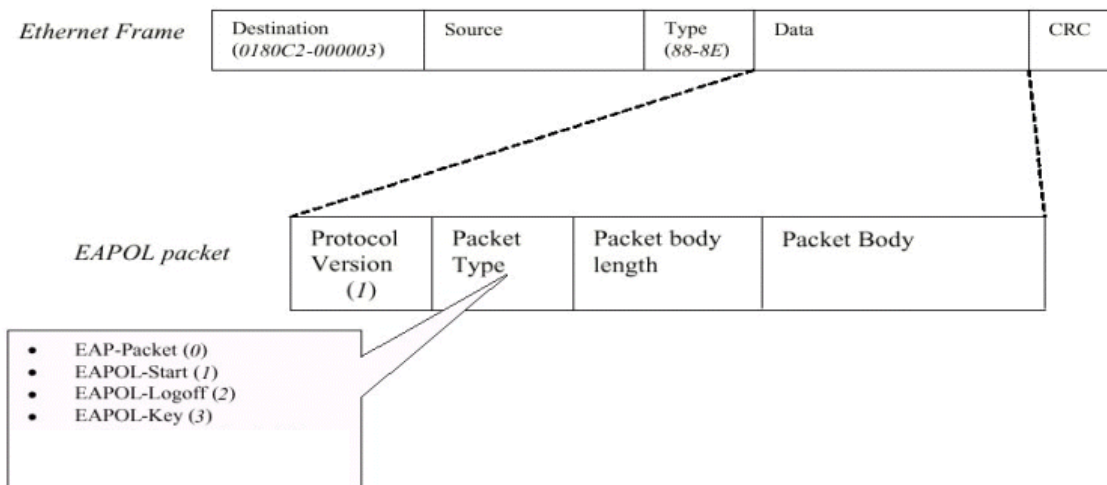
EAPOL Exchange between 802.1x Authenticator and Supplicant

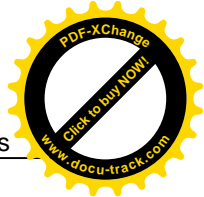
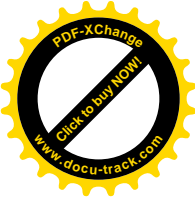
The authenticator or supplicant can initiate the authentication. If you enable the 802.1x authentication on the Wireless AP, the authenticator must initiate authentication, when it determines that the Wireless link state transits from down to up. It then sends an EAP-request/identity frame to the 802.1x 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 **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 followed:





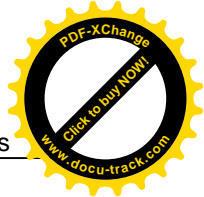
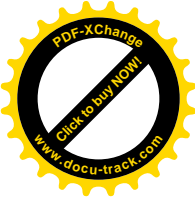
- EAP-Packet: Both the supplicant and authenticator send this packet, when the authentication is taking place. This is the packet that contains either the MD5-Challenge or TLS information required for authentication.
- EAPOL-Start: This supplicant sends this packet, when it wants to initiate the authentication 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 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 the WAP and WEP are user authentication and improved data encryption. The WAP applies the IEEE 802.1x Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can not use the P-660HW-Tx v2's local user database for WPA authentication purpose, since the local user database uses the MD5 EAP which can not generate keys.

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

If you do not have an external RADIUS 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.



Wireless Configuration

Activate the WLAN interface of the VSG1432-B101 and connect the notebook (802.11bg wireless NIC required) under the WPA-PSK as its security mode.

a. Wireless Setup.

1. Go to **Network Settings > Wireless > General.**
2. Check the **Enable** box.
3. Enter the **Network Name(SSID)**, e.g. "TEST_01".
4. Select the **Security Mode**, e.g. "WPA-PSK".
5. Enter the **Pre-Shared Key**, e.g. "11111111".
6. Select the **Encryption**, e.g. "TKIP+AES".
7. Click **Apply**.

Wireless

General | More AP | MAC Authentication | WPS | WMM | WDS | Others

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless : ☒ Enable ☐ Disable (The settings in this screen are invalid if you select this.)

Channel : Auto [more...](#)

Wireless Network Settings

Wireless Network Name(SSID): Test_01

☐ Hide SSID

☐ Client Isolation

☐ MBSSID/LAN Isolation

☐ Enhanced Multicast Forwarding

BSSID: 02:10:18:01:00:02

Security Level

No Security Basic **More Secure (Recommended)**

Security Mode: WPA-PSK

☐ Generate password automatically

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

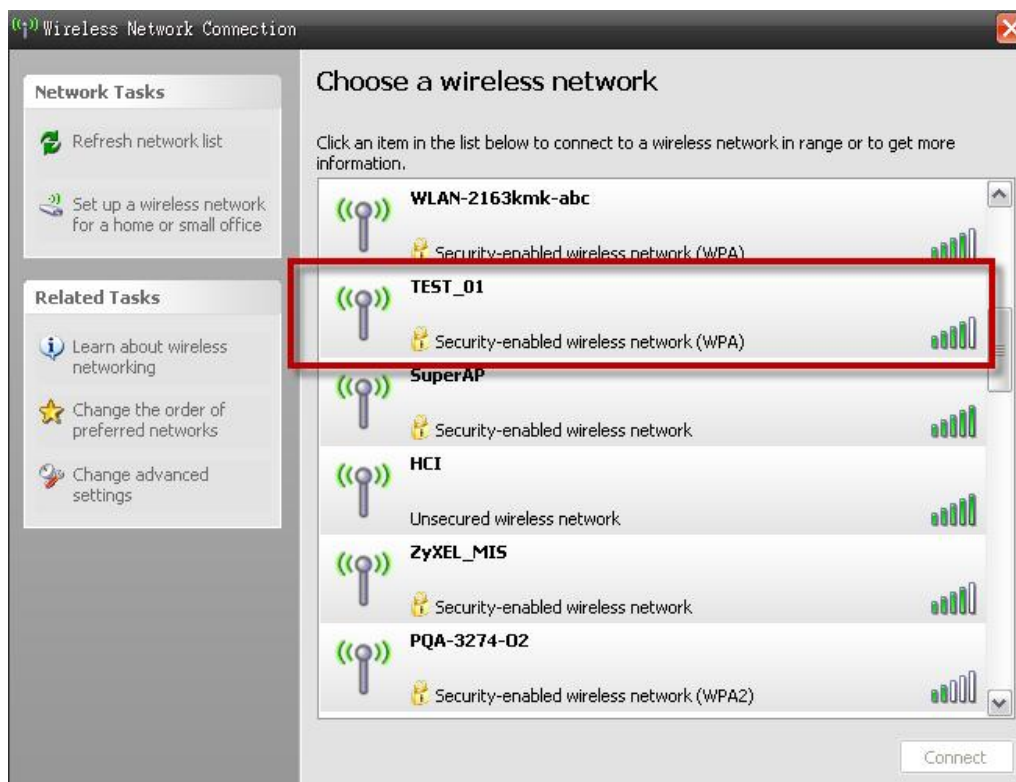
Password: [less](#)

Encryption: TKIP+AES

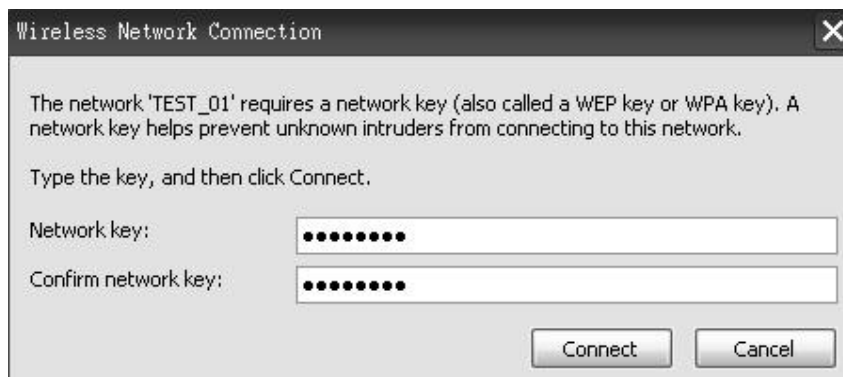
Group Key Update Timer: 1800 sec

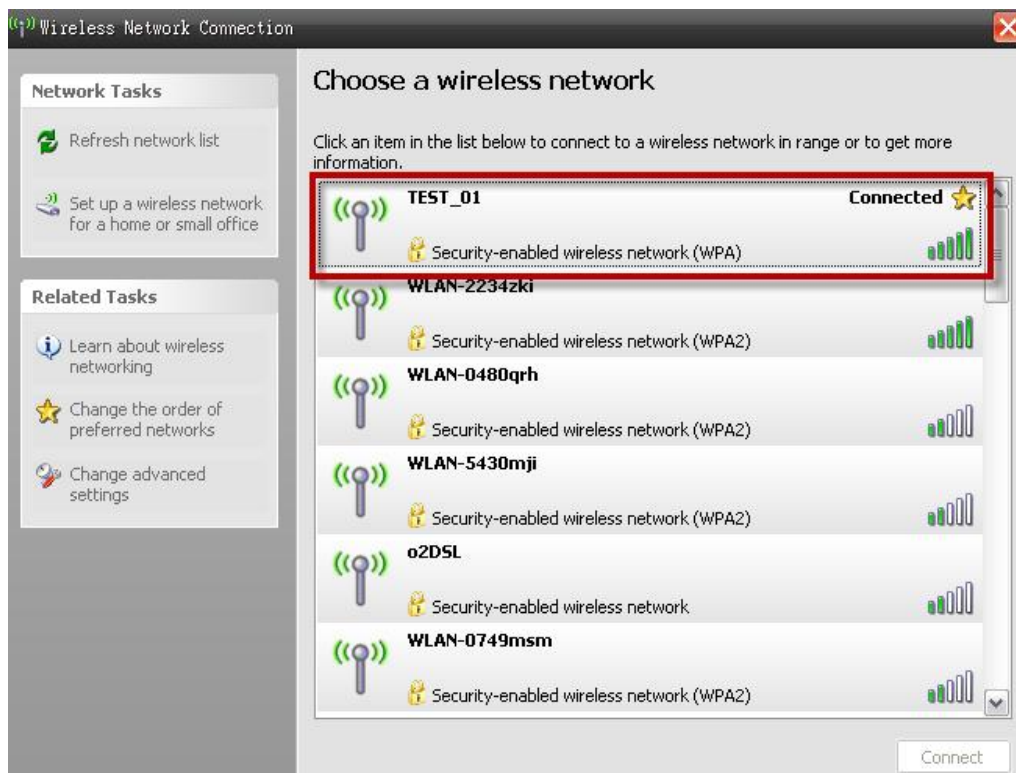
[Apply](#) [Cancel](#)

Show all the wireless networks in 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 VSG1432-B101.

b. Wireless Setup Hiding the SSID.

1. Go to **Network Settings > Wireless > General**.
2. Check the **Enable** box.
3. Enter the **Network Name(SSID)**, e.g. "TEST_01".
4. Check the **Hide Network Name(SSID)** box.
5. Select the **Security Mode**, e.g. "WPA-PSK".
6. Enter the **Pre-Shared Key**, e.g. "11111111".
7. Select the **Encryption**, e.g. "TKIP+AES".
8. Click **Apply**.

Wireless

General | More AP | MAC Authentication | WPS | WMM | WDS | Others

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless: ☒ Enable ☐ Disable (The settings in this screen are invalid if you select this.)

Channel: Auto [more...](#)

Wireless Network Settings

Wireless Network Name(SSID): Test_01

☒ Hide SSID

☐ Client Isolation

☐ MBSSID/LAN Isolation

☐ Enhanced Multicast Forwarding

BSSID: 02:10:18:01:00:02

Security Level

No Security Basic **More Secure (Recommended)**

Security Mode: WPA-PSK

☐ Generate password automatically

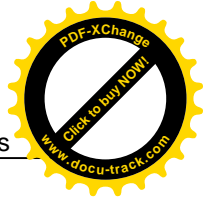
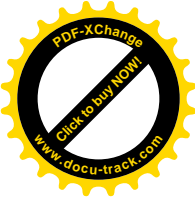
Enter 8-63 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

Password: [less](#)

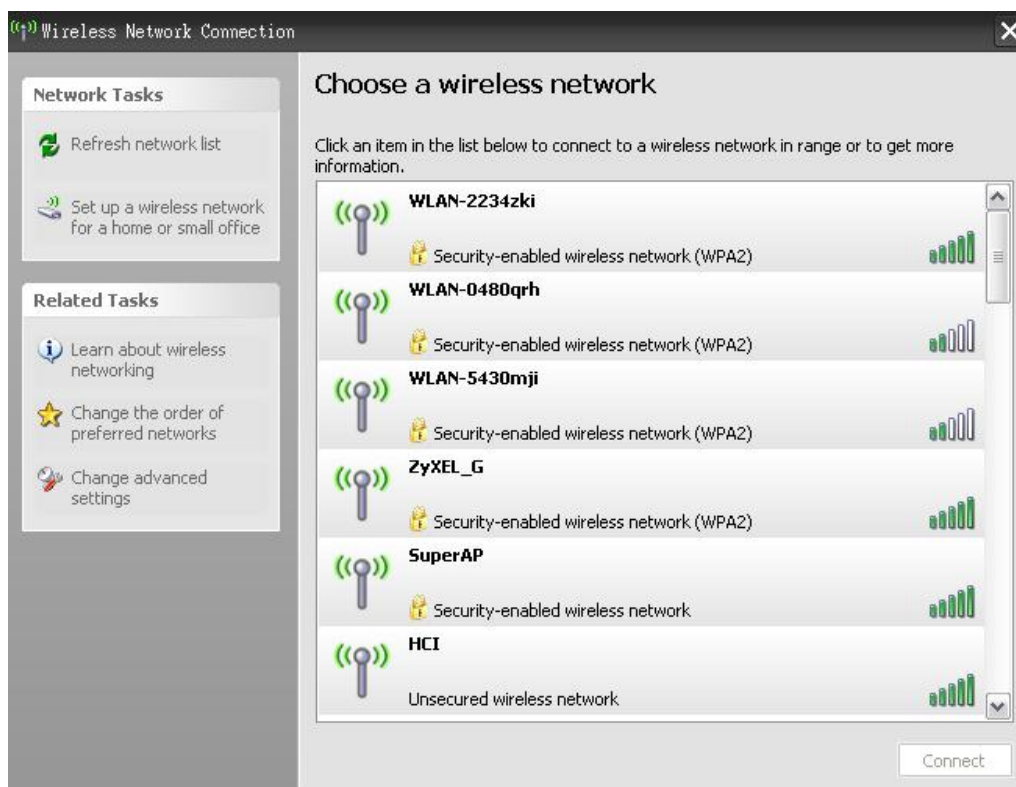
Encryption: TKIP+AES

Group Key Update Timer: 1800 sec

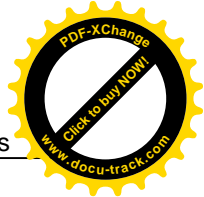
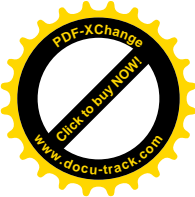
[Apply](#) [Cancel](#)



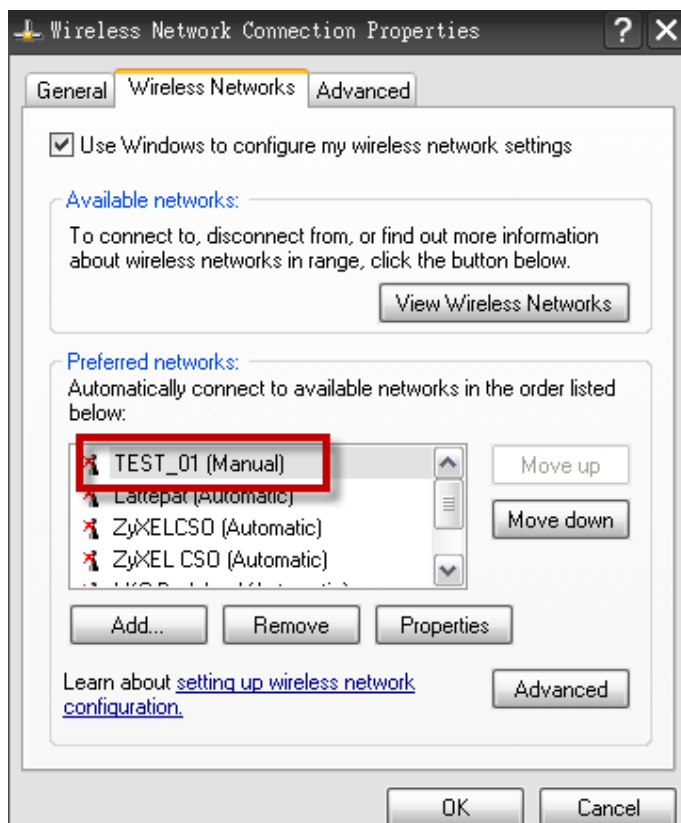
Show all the wireless networks in your notebook:

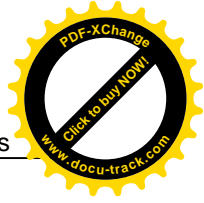


As we can see, we cannot find the SSID "TEST_01".

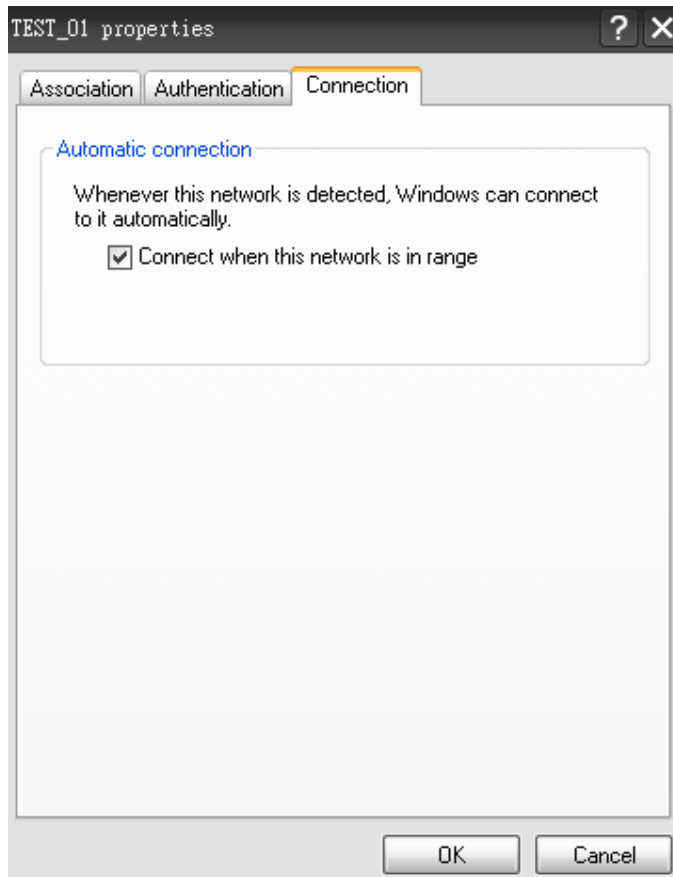


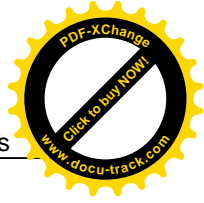
To connect to “TEST_01”, we need to configure the “Wireless Network Connection Properties” of the notebook WLAN interface:



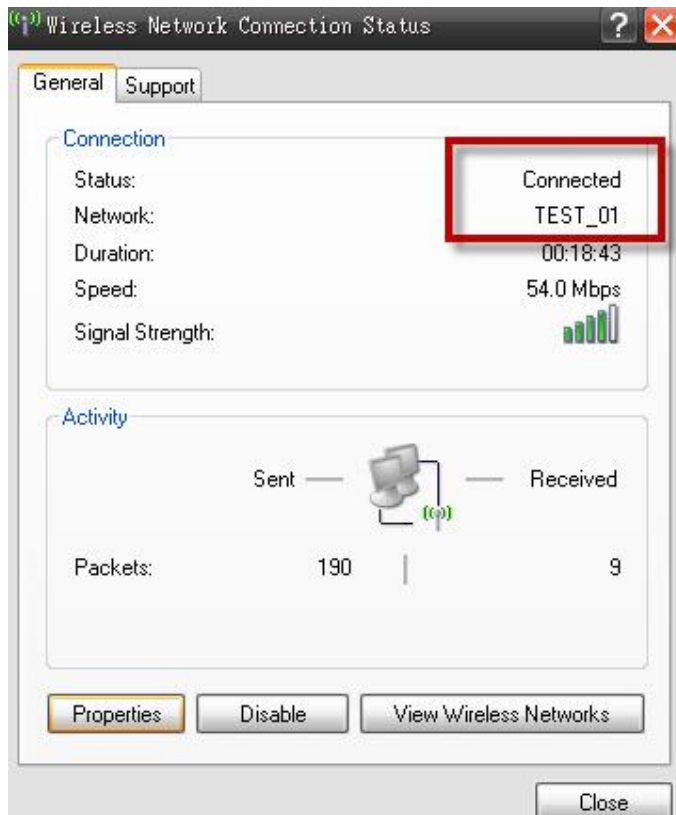


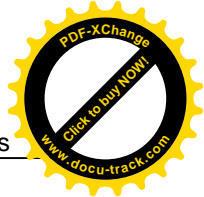
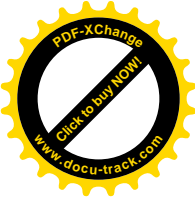
Go “Connection” tab and check the box under the name of “Connect when this network is in range”.





Then we will see the notebook connected to the “TEST_01”, even though the SSID is now displayed in the broadcast list.





c. Wireless Setup Using “Auto Generate Key”.

1. Go to **Network Settings > Wireless > General**.
2. Check the **Enable** box.
3. Check the **Generate Password Automatically** box.
4. Select the **Security Mode**, e.g. “WPA-PSK”.
5. Select the **Encryption**, e.g. “TKIP+AES”.
6. Click **Apply**.

Wireless

General | More AP | MAC Authentication | WPS | WMM | WDS | Others

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless : ☒ Enable ☐ Disable (The settings in this screen are invalid if you select this.)

Channel : [Auto](#) [more...](#)

Wireless Network Settings

Wireless Network Name(SSID):

☐ Hide SSID


☐ Client Isolation

☐ MBSSID/LAN Isolation

☐ Enhanced Multicast Forwarding

BSSID: 02:10:18:01:00:02

Security Level



Security Mode: [WPA-PSK](#)

☒ Generate password automatically

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

Password: 1B425F9823 [less](#)

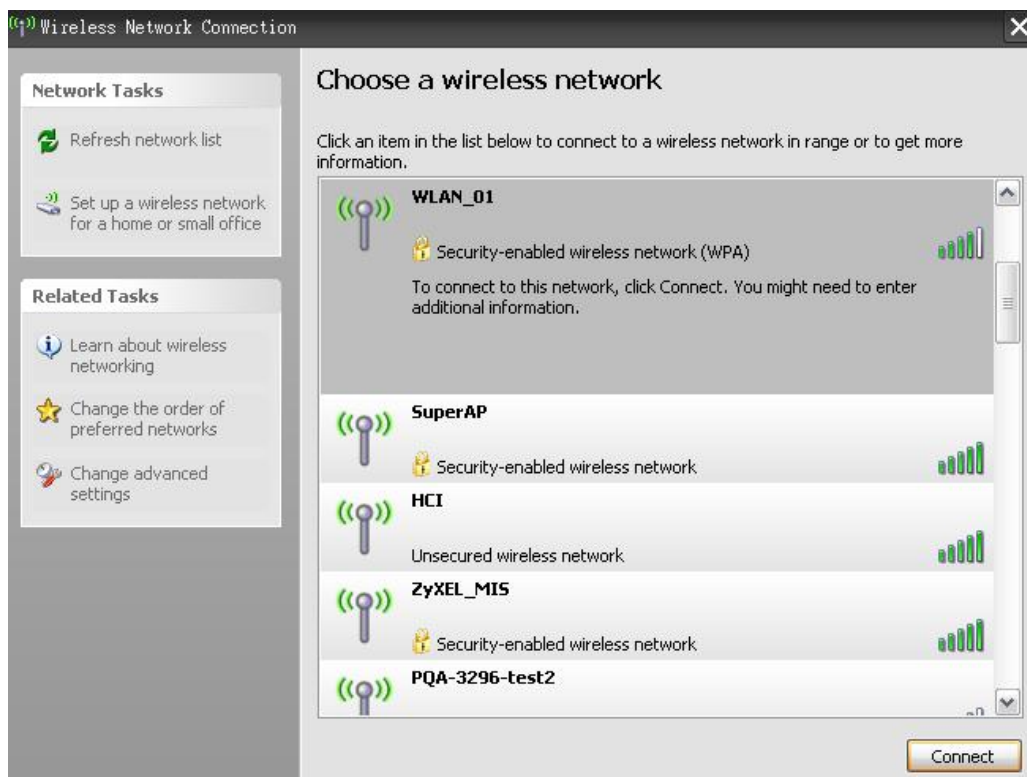
68BDDA3F57

Encryption: [TKIP+AES](#)

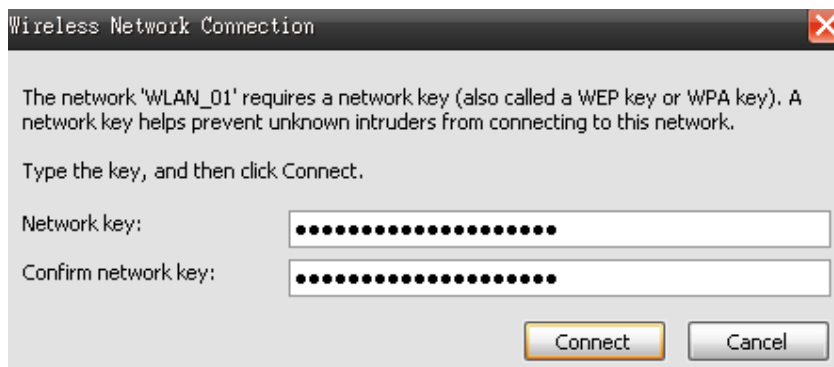
Group Key Update Timer: 1800 sec

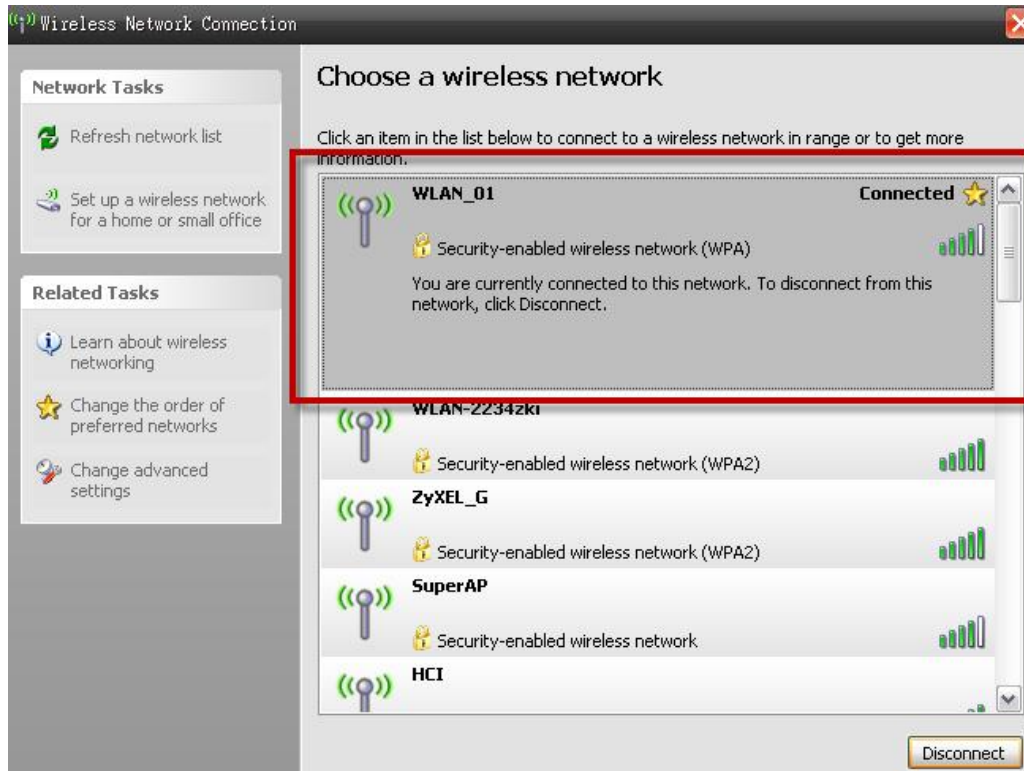
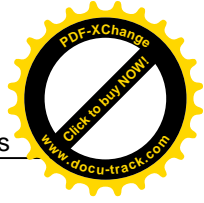
[Apply](#) [Cancel](#)

Show all the wireless networks in your notebook:

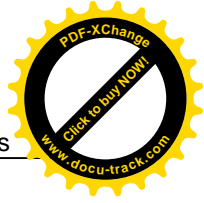


Enter the WPA-PSK pre-shared key auto-generated by VSG1432-B101.





We can see that the notebook is now connected to the WLAN interface of the VSG1432-B101.



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 calling the name **Wi-Fi Protected Setup**.

There are several different methods defined in WPS to simplify the process of configuration. VSG1432-B101 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 “push button” suffices the process to activate the security of the wireless network and at the same time be subscribed in it.

WPS configuration

a. WPS Setup

1. Go to **Network Settings > Wireless > WPS**.
2. Check the **Enable** box.
3. Click **Apply**.

Wireless

General More AP MAC Authentication **WPS** WMM WDS Others

Wi-Fi Protected Setup (WPS) lets you set up wireless security easily. Select a method for establishing a WPS connection between the router and another WPS-compatible device.

WPS Setup

WPS : ☒ Enable ☐ Disable (The settings in this screen are invalid if you select this.)

Method 1	Method 2	Method 3
<p>Push Button Configuration</p> <p>1. Click "Connect".</p> <p>Connect</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Register Wireless Client's PIN Number</p> <p>1. Enter the PIN of your wireless client and click "Register"</p> <p><input type="text"/> Register</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Enter AP's PIN Number in Wireless Client</p> <p>1. Please release configuration if you want to configure the wireless settings</p> <p>Release Configuration</p> <p>2. Enter current PIN 19951683 on your wireless client</p> <p>Generate New PIN Number</p>

b. WPS Station Setup

1. Go to **Network Settings > Wireless > WPS**.
2. Click the **Connect**.

Method 1	Method 2	Method 3
<p>Push Button Configuration</p> <p>1. Click "Connect".</p> <p>Connect</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Register Wireless Client's PIN Number</p> <p>1. Enter the PIN of your wireless client and click "Register"</p> <p><input type="text"/> Register</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Enter AP's PIN Number in Wireless Client</p> <p>1. Please release configuration if you want to configure the wireless settings</p> <p>Release Configuration</p> <p>2. Enter current PIN 19951683 on your wireless client</p> <p>Generate New PIN Number</p>

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

c. MAC filtering

1. Go to **Network Settings > Wireless > MAC Authentication**.
2. Click the **Add new MAC address** button.

The screenshot shows the 'Wireless' configuration page with the 'MAC Authentication' tab selected. The page includes a description of MAC Authentication, a dropdown for SSID (set to 'Test_01'), and radio buttons for MAC Restrict Mode (Disable, Allow, Deny). A 'MAC List' section contains an 'Add new MAC address' button and a table with columns for ID, MAC Address, and Modify. The 'Apply' and 'Cancel' buttons are at the bottom right.

Wireless

General More AP **MAC Authentication** WPS WMM WDS Others

MAC Authentication can allow or block a device(s) from accessing your wireless network. Edit the table below to add MAC addresses that you want to allow or deny.

SSID : Test_01

MAC Restrict Mode : ☒ Disable ☐ Allow ☐ Deny

MAC List

Add new MAC address

#	MAC Address	Modify
---	-------------	--------

Apply Cancel

3. Enter the **MAC Address**, e.g. "00:12:F0:E3:94:5C".
4. Click **Apply**.

The screenshot shows the 'MAC Filter Configuration' dialog box. It has a title bar with a close button. The main content area is titled 'Add to list by MAC address' and contains the instruction 'To add a device, please enter device's MAC address :'. Below this is a form with six input fields for the MAC address, pre-filled with '00', '12', 'F0', 'E3', '94', and '5C'. The 'Apply' and 'Cancel' buttons are at the bottom right.

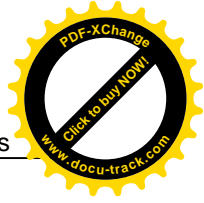
MAC Filter Configuration

Add to list by MAC address

To add a device, please enter device's MAC address :

00 : 12 : F0 : E3 : 94 : 5C

Apply Cancel



Product FAQ

Will the device work with my Internet connection?

VSG1432-B101 is designed to be compatible with major ISPs utilize VDSL as a broadband service. VSG1432-B101 offers Ethernet ports to connect to your computer so the device is placed in the line between the computer and your ISP. If your ISP supports PPPoE you can also use the device, because PPPoE is supported in the device.

Why do I need to use VSG1432-B101?

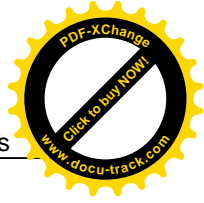
You need a VDSL modem/router to use with VDSL line, VSG1432-B101 is an ideal device for such application. The device has 4 Ethernet ports (LAN ports) and one VDSL WAN port. You should connect the computer to the LAN port and connect the VDSL line to the WAN port. If the ISP uses PPPoE you need the user account to access Internet.

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 device, please make sure your ISP supports PPPoE.

Does the device support PPPoE?

Yes. The device 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 device 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 device?

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

How can I configure the device?

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

What network interface does the device support?

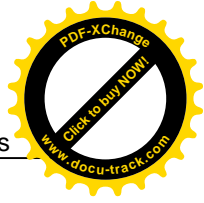
The device supports 10/100M Ethernet to connect to the LAN computer or hub/switch and an up to 100M VDSL interface to the ISP.

What can we do with the device?

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 device.

Does device support dynamic IP addressing?

The device 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 is 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 route between the virtual IP and the real IP.

How does e-mail work through the device?

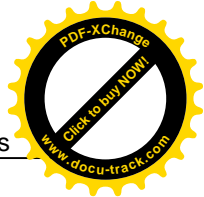
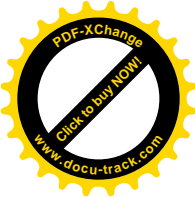
It depends on what kind of IP you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through the device using jane@mycompany.com and debbie@mycompany.com 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 the device 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.

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

Yes, it is possible because the device 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.

**What DHCP capability does the device support?**

The device supports DHCP client (Ethernet encap) 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 use 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 used the reset button, more over what field of parameter will be reset by reset button?

You can used a sharp pointed object insert it into the little reset hole beside the power connector. Press down the reset button and hold down for approx 5 second, the unit will be reset. When the reset button is pressed the devices all parameter will be reset back to factory default include, password, and IP address.

The default IP address is 192.168.1.1, Password 1234.

What network interface does the new device series support?

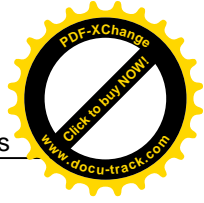
The new device series support auto MDX/MDIX 10/100M Ethernet LAN port to connect to the computer or Switch on LAN.

How does the device support TFTP?

In addition to the direct console port connection, the device supports the uploading/download of the 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.



How fast can the data go?

The speed of the VDSL 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 100 Mbps.

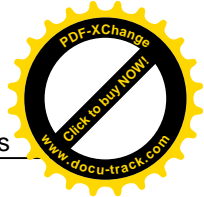
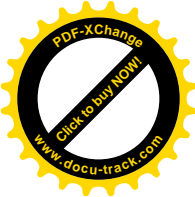
To create the appearance of faster network access, service companies plan to store or "cache" frequently requested web sites and Usenet newsgroups on a server at their head-end. Storing data locally will remove some of the bottleneck at the backbone connection.

How fast can they go? In a perfect world (or lab) they can receive data at speeds up to 100 Mbps. In the real world, with cost conscious cable companies running the systems, the speed will probably fall behind the speed that the ISP appointed at the first place.

What is Multi-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 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 incoming packets back into local IP addresses. The IP addresses for the 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, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the device, thus preventing intruders from probing your network.

The SUA feature that the device supports previously operates by mapping the private IP addresses to a global IP address. It is only one subset of the NAT. The device supports most of the features of the NAT based on RFC 1631, and we call this feature as '**Multi-NAT**'. For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

**When do I need Multi-NAT?**

- a. Make local server accessible from outside 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.

- a. Support Non-NAT Friendly Applications

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

What IP/Port mapping does Multi-NAT support?

NAT supports five types of IP/port mapping. They are: One to One, Many to One, Many to Many Overload, Many to Many No Overload and Server. The details of the mapping between ILA and IGA are described as below. Here we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA),

1. **One to One**

In One-to-One mode, the device maps one ILA to one IGA.

2. **Many to One**

In Many-to-One mode, the device maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

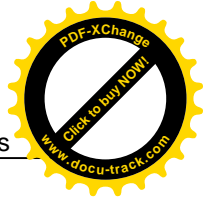
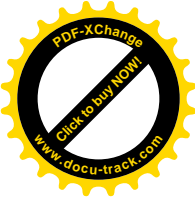
3. **Many to Many Overload**

In Many-to-Many Overload mode, the device maps the multiple ILA to shared IGA.

4. **Many to Many No Overload**

In Many-to-Many No overload mode, the device maps each ILA to unique IGA.

5. **Server**



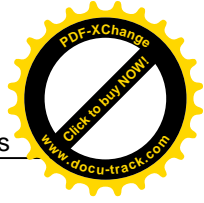
In Server mode, the device maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note: if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many-to-Many No Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

What is the difference between SUA and Multi-NAT?

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. The device now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple servers of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions that supported SUA 'visible' servers had to be of different types. The device supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The device supports 2 sets since there is only one remote node. The default SUA (Read Only) is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions.

**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 device 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?

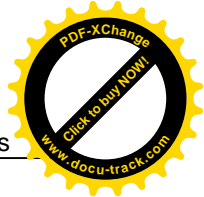
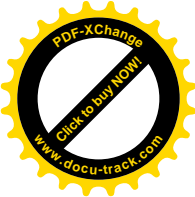
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as WWW.DYNDNS.ORG.

Without DDNS, we always tell the users to use the WAN IP of the 312 to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the device, 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 312.

When the ISP assigns the device a new IP, the device 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 device sends this IP to the DDNS server for its updates.



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:

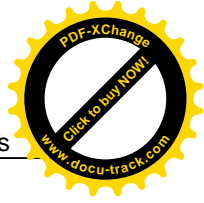
Wireless technology allows the network to go where wire cannot go.

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?

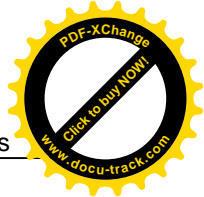
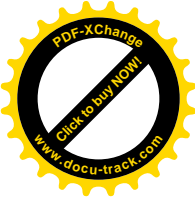
The AP (access point also known as a base station) is the wireless server that with an antenna and a wired Ethernet connection that broadcasts information using radio signals. AP typically act as a bridge for the clients. It can pass information to wireless LAN cards that have been installed in computers 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?

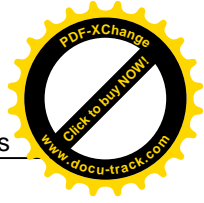
802.11a the second revision of 802.11 that operates in the unlicensed 5 GHz band and allows transmission rates of up to 54Mbps. 802.11a uses OFDM (orthogonal frequency division multiplexing) as opposed to FHSS or DSSS. Higher data rates are possible by combining channels. Due to higher frequency, range 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.

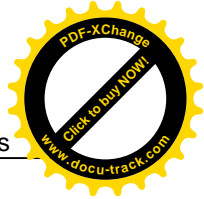
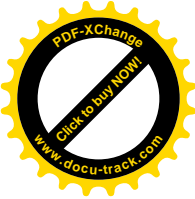
Does the 802.11 interfere with Bluetooth devices?

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 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 a high water content do not allow radio waves to pass through. Metals reflect radio waves and concrete attenuates radio waves. The amount of attenuation suffered in passing through concrete will be a function of its thickness and amount of metal re-enforcement used.



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.

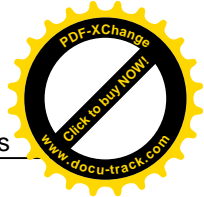
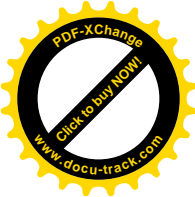
WWANs are generally publicly shared data networks designed to provide coverage in metropolitan areas and along traffic corridors. WWANs are owned by a service provider or carrier. Data rates are low and charges are based on usage. Specialized applications are characteristically designed around short, 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)?

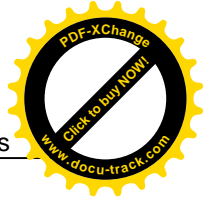
FHSS uses a narrowband carrier which hops through a predefined sequence of several frequencies at a specific rate. This avoids problems with fixed channel narrowband noise and simple jamming. Both transmitter and receiver must have their hopping sequences synchronized to create the effect of a single "logical channel". To an 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 2.4GHz 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?

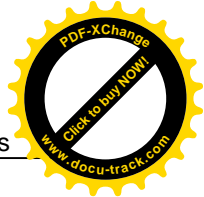
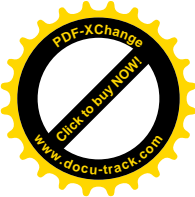
Enable Wired Equivalency Protocol (WEP) or Wi-Fi Protected Access (WPA) to encrypt the payload of packets sent across a radio link.

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 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.

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

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?

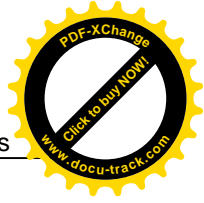
Many APs by default have broadcasting the SSID turned on. Sniffers typically will find the SSID in the broadcast beacon packets. Turning off the broadcast of SSID in the beacon message (a common practice) does not prevent getting the SSID; since the SSID is sent in the clear in the probe message when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

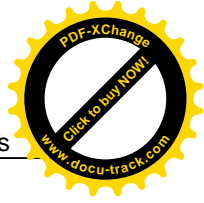
IEEE 802.1x Port-Based Network Access Control is an IEEE (Institute of Electrical and Electronics Engineers) standard, which specifies a standard mechanism for authenticating, at the link layer (Layer 2), users' access to IEEE 802 networks such as Ethernet (IEEE 802.3) and Wireless LAN (IEEE 802.11).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

What is the difference between 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?

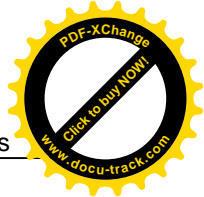
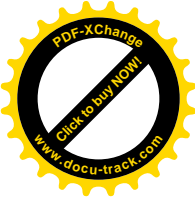
RADIUS stands for Remote Authentication Dial-In User Service. RADIUS is a standard that has been implemented into several software packages and networking devices. It allows user information to be sent to a central database running on a RADIUS Server, where it is verified. RADIUS also provides a mechanism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

What is WPA?

WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i security specification draft. Key difference 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 user does not have a Radius server but still wants to benefit from it. Because WPA-PSK only requires a single password to be entered on wireless AP/gateway and wireless client. As long as the passwords match, a client will be granted access to the WLAN.



Trouble Shooting

In case of problems happening to the VSG1432-B101, we are able to check the device with more detailed information by entering the “shell mode”. Those statistics may help the engineer to pinpoint the problem more easily.

How to enter the “Shell mode”

Login to the device by telnet

Execute “sh”

```
ZyXEL xDSL Router
Login: 1234
Password:
> sh

BusyBox v1.00 (2009.01.14-02:33+0000) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

#
```

CPU usage

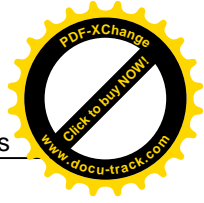
Command:

#top

```
Mem: 21512K used, 7784K free, 0K shrd, 2076K buff, 7608K cached
Load average: 0.11, 0.08, 0.08 (State: S=sleeping R=running, W=waiting)

  PID USER      STATUS  RSS    PPID  %CPU  %MEM  COMMAND
12404 1234        R       324   12323  0.1   1.1   exe
  114 1234        S      1680    113  0.0   5.7   ssk
  326 1234        S      1368    113  0.0   4.6   wlmngr
12320 1234        S       612    113  0.0   2.0   telnetd
12321 1234        S       564  12320  0.0   1.9   telnetd
  113 1234        S       548     54  0.0   1.8   smd
  412 1234        S       488     1  0.0   1.6   nas
  706 1234        S       480    113  0.0   1.6   pppd
 1003 1234        S       400    113  0.0   1.3   ripd
  246 1234        S       388    113  0.0   1.3   dhcpd
   54 1234        S       360     1  0.0   1.2   sh
12323 1234        S       352  12322  0.0   1.2   exe
 1002 1234        S       348    113  0.0   1.1   zebra
  932 1234        S       332    113  0.0   1.1   igmp
12322 1234        S       320  12321  0.0   1.0   sh
   1 1234        S       316     0  0.0   1.0   init
  949 1234        S       296    113  0.0   1.0   dnstproxy
  913 1234        S       272    113  0.0   0.9   dhcpc
   42 1234        SW      0       1  0.0   0.0   ntdblockd
   3 1234        SW<      0       1  0.0   0.0   events/0
```

(press Ctrl+C to exit)

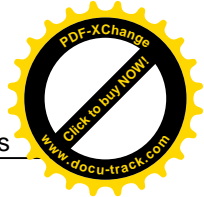
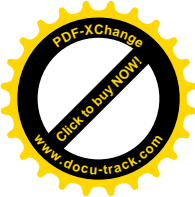


Memory usage

Command:

cat /proc/meminfo

```
# cat /proc/meminfo
MemTotal:      29296 kB
MemFree:       7748 kB
Buffers:       2076 kB
Cached:        7608 kB
SwapCached:    0 kB
Active:        6004 kB
Inactive:      5808 kB
SwapTotal:     0 kB
SwapFree:      0 kB
Dirty:         0 kB
Writeback:     0 kB
AnonPages:     2140 kB
Mapped:        2432 kB
Slab:          7784 kB
SReclaimable:  404 kB
SUnreclaim:    7380 kB
PageTables:    256 kB
NFS_Unstable:  0 kB
Bounce:        0 kB
CommitLimit:   14648 kB
Committed_AS:  5176 kB
UmallocTotal: 1032148 kB
UmallocUsed:   1708 kB
UmallocChunk: 1029524 kB
#
```

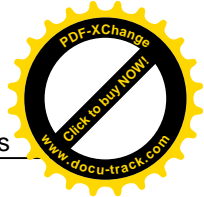
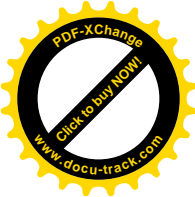


Current processes

Command:

#ps

```
# ps
  PID  Uid        VmSize  Stat Command
    1  1234          316  S    init
    2  1234          SWN [ksoftirqd/0]
    3  1234          SW< [events/0]
    4  1234          SW< [khelper]
    5  1234          SW< [kthreadd]
   14  1234          SW< [kblockd/0]
   28  1234          SW  [pdflush]
   29  1234          SW  [pdflush]
   30  1234          SW< [kswapd0]
   31  1234          SW< [aio/0]
   42  1234          SW  [mtdblockd]
   54  1234         360  S    -sh
   96  1234          SW  [bcmssl]
  113  1234         548  S    smd
  114  1234        1680  S    ssk
  246  1234         388  S    dhcpd
  326  1234        1368  S    wlmngr -m 0
  412  1234         488  S    nas -P /var/wl0nas.lan0.pid -H 34954 -l br0 -i wl0 -A
  706  1234         480  S    pppd -c ppp0.100 -i ptm0.100 -u test -p ***** -f 0
  913  1234         272  S    dhcpc -f -i ptm0.200
  932  1234         332  S    igmp ptm0.200
  949  1234         296  S    dnsproxy -D Home
 1002  1234         348  S    zebra -f /var/zebra/zebra.conf
 1003  1234         400  S    ripd -f /var/zebra/ripd.conf
12320 1234         612  S    telnetd
12321 1234         564  S    telnetd
12322 1234         320  S    sh -c sh
12323 1234         356  S    sh
12678 1234        300  R    ps
#
```

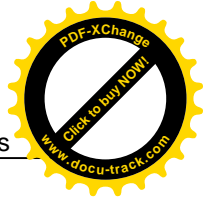
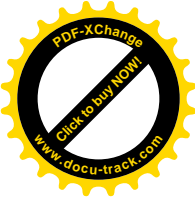


NAT session table

Command:

```
#cat /proc/net/ip_conntrack
```

```
# cat /proc/net/ip_conntrack
tcp      6 424835 ESTABLISHED src=10.59.1.47 dst=172.23.5.49 sport=1526 dport=11
35 [UNREPLIED] src=172.23.5.49 dst=10.59.1.47 sport=1135 dport=1526 use=1
unknown  2 543 src=172.26.208.34 dst=224.0.0.22 [UNREPLIED] src=224.0.0.22 dst=1
72.26.208.34 use=1
tcp      6 424838 ESTABLISHED src=10.59.1.47 dst=172.23.5.50 sport=1514 dport=11
86 [UNREPLIED] src=172.23.5.50 dst=10.59.1.47 sport=1186 dport=1514 use=1
unknown  2 598 src=10.0.0.33 dst=224.7.7.7 [UNREPLIED] src=224.7.7.7 dst=10.0.0.
33 use=1
udp      17 29 src=172.26.208.1 dst=224.0.0.9 sport=520 dport=520 [UNREPLIED] sr
c=224.0.0.9 dst=172.26.208.1 sport=520 dport=520 use=1
tcp      6 421514 ESTABLISHED src=10.59.1.47 dst=172.23.5.2 sport=3698 dport=102
6 [UNREPLIED] src=172.23.5.2 dst=10.59.1.47 sport=1026 dport=3698 use=1
udp      17 88 src=172.26.208.35 dst=168.95.1.1 sport=60320 dport=53 [UNREPLIED]
src=168.95.1.1 dst=172.26.208.35 sport=53 dport=60320 use=1
udp      17 88 src=172.26.208.35 dst=172.23.5.1 sport=60320 dport=53 [UNREPLIED]
src=172.23.5.1 dst=172.26.208.35 sport=53 dport=60320 use=1
udp      17 29 src=172.26.208.35 dst=224.7.7.7 sport=2503 dport=1234 [UNREPLIED]
src=224.7.7.7 dst=172.26.208.35 sport=1234 dport=2503 use=1
tcp      6 421649 ESTABLISHED src=10.59.1.47 dst=64.15.120.162 sport=3720 dport=
80 [UNREPLIED] src=64.15.120.162 dst=10.59.1.47 sport=80 dport=3720 use=1
tcp      6 424921 ESTABLISHED src=10.59.1.47 dst=64.15.120.162 sport=1590 dport=
80 [UNREPLIED] src=64.15.120.162 dst=10.59.1.47 sport=80 dport=1590 use=1
tcp      6 424923 ESTABLISHED src=10.59.1.47 dst=172.23.5.49 sport=1589 dport=11
35 [UNREPLIED] src=172.23.5.49 dst=10.59.1.47 sport=1135 dport=1589 use=1
unknown  2 598 src=10.0.0.33 dst=224.8.8.8 [UNREPLIED] src=224.8.8.8 dst=10.0.0.
33 use=1
```

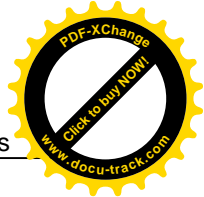
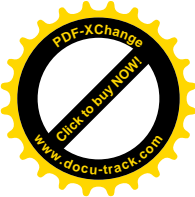


IGMP table

Command:

```
#cat /proc/net/igmp
```

# cat /proc/net/igmp								
Idx	Device	:	Count	Querier	Group	Users	Timer	Reporter
1	lo	:	0	U2				
		:		E0000001	1	0:00000000		0
2	ifb0	:	1	U2				
		:		E0000001	1	0:00000000		0
3	eth0	:	1	U2				
		:		E0000001	1	0:00000000		0
9	eth1	:	1	U2				
		:		E0000001	1	0:00000000		0
10	eth2	:	1	U2				
		:		E0000001	1	0:00000000		0
11	eth3	:	1	U2				
		:		E0000001	1	0:00000000		0
12	wl0	:	1	U2				
		:		E0000001	1	0:00000000		0
13	br0	:	4	U2				
		:		E0000009	1	0:00000000		0
		:		E0000016	1	0:00000000		1
		:		E0000002	1	0:00000000		1
		:		E0000001	1	0:00000000		0
19	ptm0	:	6	U2				
		:		E0000001	1	0:00000000		0
20	ptm0.100	:	1	U2				
		:		E0000001	1	0:00000000		0
21	ppp0.100	:	0	U2				
		:		E0000001	1	0:00000000		0
22	ptm0.200	:	6	U2				
		:		FFFFFFFA	1	0:00000000		1
		:		E0000009	1	0:00000000		0
		:		E0090909	1	0:00000000		1
		:		E0080808	1	0:00000000		1
		:		E0070707	1	0:00000000		1
		:		E0000001	1	0:00000000		0
#								

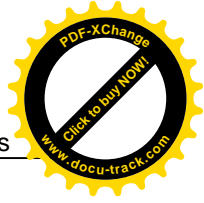


Packets statistics

Command:

#cat /proc/net/dev

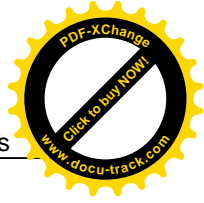
```
# cat /proc/net/dev
Inter-|   Receive                                           |   Transmit
face |bytes  packets errs drop fifo frame compressed multicast|bytes  packets
-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----
lo:    7736      92      0      0      0      0      0      0      0      7736
92      0      0      0      0      0      0      0      0      0
ifb0: 4043846    3729      0      0      0      0      0      0      0 4043846    3729
29      0      0      0      0      0      0      0      0      0
ifb1:      0      0      0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0      0
ds10:      0      0      0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0      0
bcm5w:56914755  58830      0      0      0      0      0      0      0 1457217511 1091888
1888      0      0      0      0      0      0      0      0      0
pktcmf_sw_sar:      0      0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0      0
pktcmf_sar_sw:      0      0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0      0
eth0: 400970    5867      0      0      0      0      0      0      0 1441674402 1050331
0331      0      0      0      0      0      0      0      0      0
eth1:      0      0      0      0      0      0      0      0      0      0
35      0      0      0      0      0      0      0      0      0
eth2:56513785  52963      0      0      0      0      0      0      0 15363797 39289
89      0      0      0      0      0      0      0      0      0
eth3:      0      0      0      0      0      0      0      0      0      0
33      0      0      0      0      0      0      0      0      0
wl0:      0      0      0      0      0      0 34706      0      0      0
0      19      0      0      0      0      0      0      0      0
br0: 6048351    26378      0      0      0      0      0      0      0 6534 1448441607 1068670
8670      0      0      0      0      0      0      0      0      0
wl0.1:      0      0      0      0      0      0 34706      0      0      0
0      19      0      0      0      0      0      0      0      0
wl0.2:      0      0      0      0      0      0 34706      0      0      0
0      19      0      0      0      0      0      0      0      0
wl0.3:      0      0      0      0      0      0 34706      0      0      0
0      19      0      0      0      0      0      0      0      0
ptm0:1446356465 1073793      0      0      0      0      0      0      0 1049839      0 40564
0564      0      0      0      0      0      0      0      0      0
ptm0.100: 344990    2601      0      0      0      0      0      0      0 136016
1623      0      0      0      0      0      0      0      0      0
ppp0.100: 298339    2197      0      0      0      0      0      0      0 90399
1236      0      0      0      0      0      0      0      0      0
ptm0.200:1427016925 1050776      0      0      0      0      0      0      0 1049647 4065259
3827      0      0      0      0      0      0      0      0      0
```

**Physical layer statistics**

Command:

#adslctl info

```
# adslctl info
adslctl: ADSL driver and PHY status
Status: Showtime
Retrain Reason: 0
Max:   Upstream rate = 59659 Kbps, Downstream rate = 151768 Kbps
Path:  0, Upstream rate = 45054 Kbps, Downstream rate = 100015 Kbps
```



CLI Command List

The latest CI command list is available in release notes of every ZyXEL firmware release.

Please go to ZyXEL public WEB site http://www.zyxel.com/web/support_download.php to download firmware package (*.zip), you should unzip the package to get the release note in PDF format.