SBG3500-N000

Wireless N Fiber WAN Small Business Gateway

Version 1.00
Edition 2, 4/2014

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the SBG3500-N000 and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

Contents Overview

Table of Contents

PART I
User's Guide

Introducing the SBG3500-N

1.1 Overview

The SBG3500-N is a secure VPN (Virtual Private Network), multi-WAN gateway that provides high-speed Internet access for business users. It features not only VDSL2/ADSL2+ Bonding functionality, but also one Gigabit Ethernet (GbE) WAN with Small Form Factor Pluggable (SFP) interface. SFP is also known as Fiber Optics interface. The GbE WAN with SFP is a dual-personality design (GbE + Fiber) which enables increased bandwidth and extended coverage. Namely, the SBG3500-N can adopt varied network environment and enable service providers to flexibly install this device for VDSL, Fiber and 3G, in addition to provide load-balancing to ensure seamless Internet connectivity.

FEATURES

- Four GbE Ports for LAN Connection
- One USB Port for 3G Connection and File Sharing
- One SFP Port for Fiber Optic Internet Connection
- One GbE WAN Port
- Two VDSL2/ADSL2+ Integrated Ports (Bonding)
- Integrated Firewall with Secure Network Management
- IP secure VPN

Only use firmware for your SBG3500-N's specific model. Refer to the label on the bottom of your SBG3500-N.

Note: SFP and GbE connections cannot be used at the same time.

1.2 Applications for the SBG3500-N

Here are some example uses for which the SBG3500-N is well suited.

1.2.1 Internet Access

Your SBG3500-N provides multiple Internet access methods (up to two at a time), and you can use them in the following combinations, if your ISP supports them.

- ADSL2+ and VDSL, connect the DSL1 and/or DSL2 port using a phone cable to a DSL or MODEM on a splitter or your telephone jack. For single DSL connection, use only DSL1 port. For DSL bonding connection, use both DSL1 and DSL2 port at the same time. Refer to Section 6.2 on page 106 for the **Network Setting > Broadband** screen. When using the DSL1/DSL2 ports and VDSL connection is not available, then the ADSL2+ will automatically be the network interface.
- DSL and GbE, connect the DSL port to the DSL or MODEM as described above and connect the GbE port to a broadband router (if available) using an Ethernet cable. The 3G USB dongle is the failover or a backup connection in case both the DSL and GbE fails. You can set the load balance and failover in SBG3500-N to prioritize and redirect all traffic to the backup connection in case the Internet access is down by clicking **Network Settings** > **Broadband** > **Multi-WAN**
- DSL and Fiber (SFP), connect the the DSL port to the DSL or MODEM and connect the SFP port using a Fiber Optical module, also known as a mini-GBIC transceiver, to a Switch or Router. The 3G USB dongle is the failover or backup connection. Set load balance as described above and see the SBG3500-N's Quick Start Guide for details on how to install and remove a mini-GBIC transceiver.
- DSL and 3G, connect the DSL port to the DSL or MODEM and connect the USB port using a USB 3G dongle. The Fiber/Ethernet is the failover. You can set the load balance/failover as described above.
- Fiber and 3G, connect the SFP port using a mini-GBIC transceiver and the USB port using a USB 3G dongle as described above. The DSL is the failover in case both Fiber and 3G is unavailable.
- GbE and 3G, connect the GbE port to a broadband router and the USB port using a USB 3G dongle. The DSL is the failover in case both Fiber and 3G is unavailable.
- WLAN or Wireless Internet access, Refer to Section 1.2.2 on page 20 for more information.

The below table is a summary of the SBG3500-N Multi-WAN combinations and failover.

DSL	SFP/ETHERNET WAN	3G
Active	Active	Failover
Active	Failover	Active
Failover	Active	Active

The following figure shows the possible internet access scenarios described above.

Computers can connect to the SBG3500-N’s LAN ports (or wirelessly).

Figure 1 SBG3500-N’s Internet Access Application

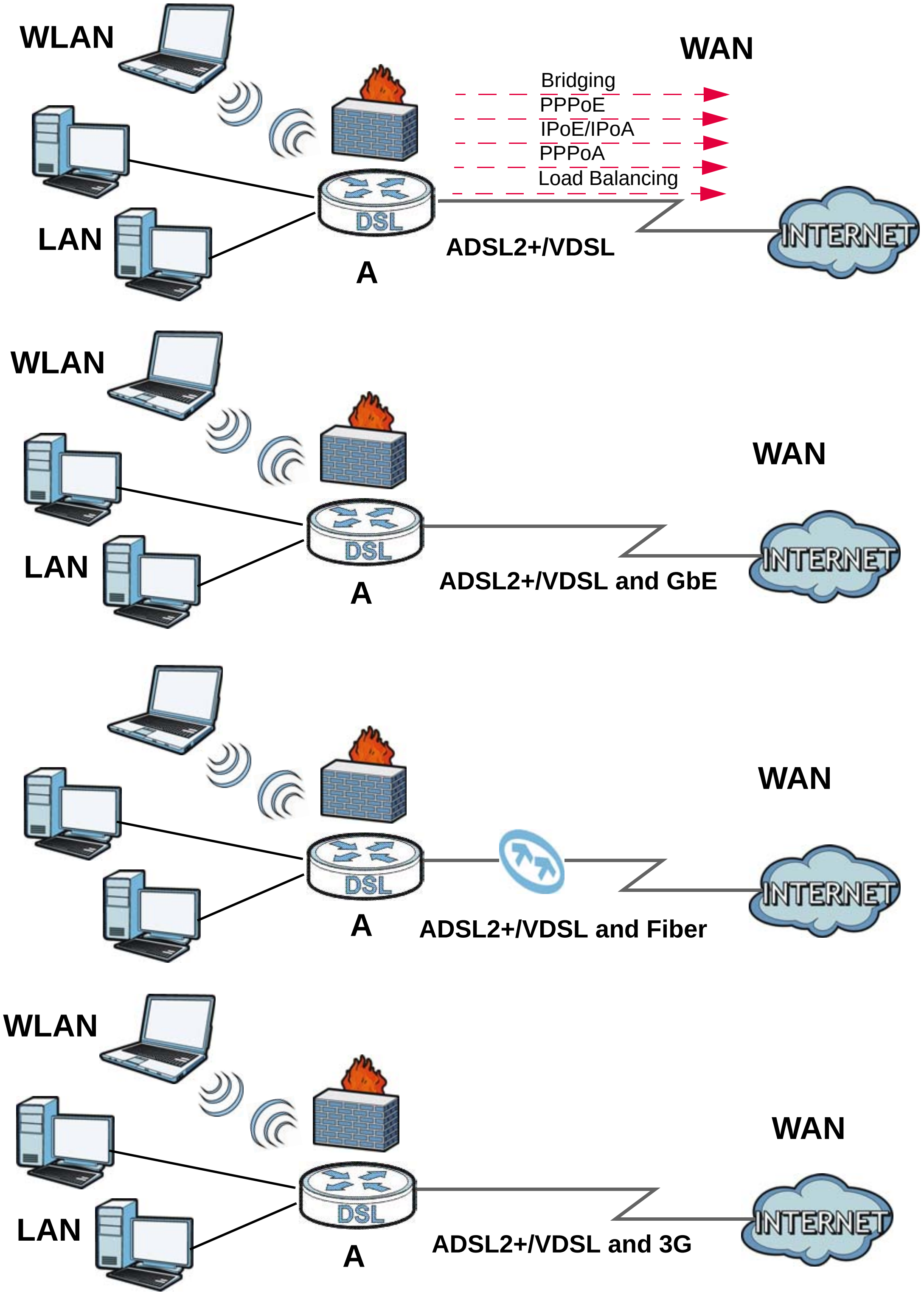
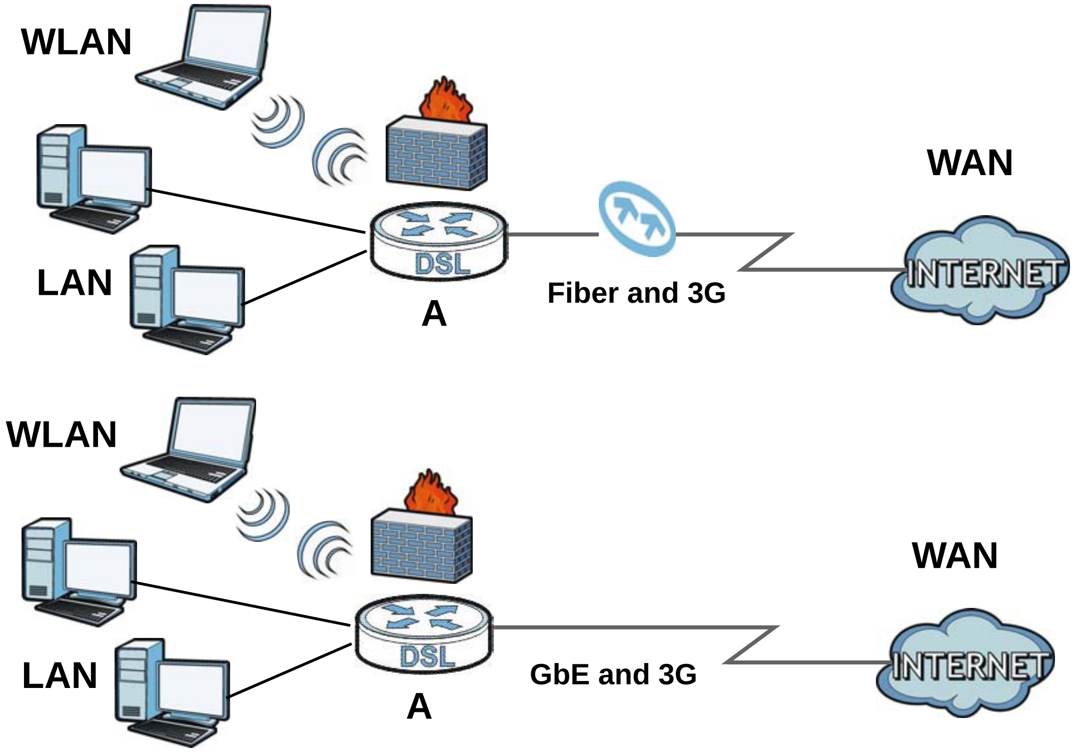


Figure 2 SBG3500-N's Internet Access Application (Continue)



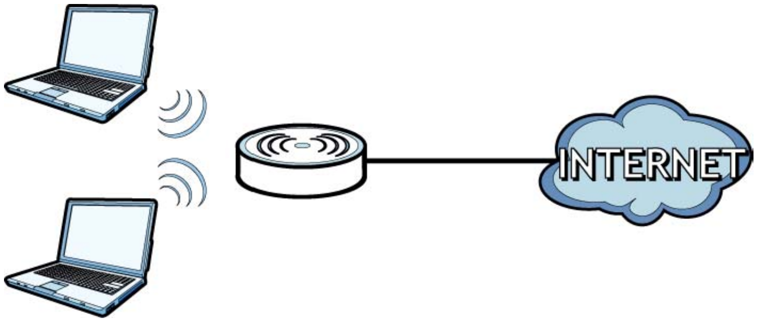
You can also configure IP filtering on the SBG3500-N for secure Internet access. Go to **Security** > **MAC Filter** to do this task. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

1.2.2 Wireless LAN

The SBG3500-N is a wireless Access Point (AP) for wireless clients, such as notebook computers or PDAs and iPads. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

You can configure your wireless network in either the built-in Web Configurator.

Figure 3 Wireless Access Example



Using the WLAN Button

If the wireless network is turned off, press the **WLAN** button at the back of the SBG3500-N. Once the **WLAN** LED turns green, the wireless network is active.

1.2.3 SBG3500-N's USB Support

The USB port of the SBG3500-N is used for 3G Dongle and file-sharing.

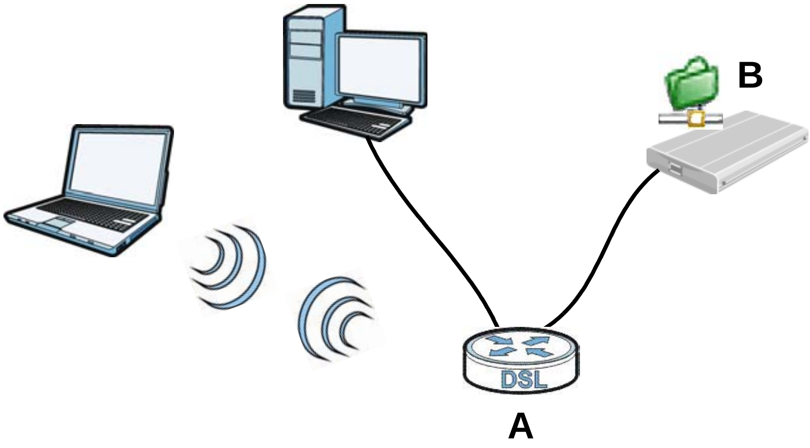
3G Dongle

See the product page on ZyXEL's website for the list of 3G Dongles that are compatible. To set up a new 3G Dongle, click **Network Settings** > **Broadband** > **3G WAN**, and to add new 3G Dongle, click **Network Settings** > **Broadband** > **Add new 3G Dongle**.

File Sharing

Use the built-in USB 2.0 port to share files on a USB memory stick or a USB hard drive (**B**). You can connect one USB hard drive to the SBG3500-N at a time. Use FTP to access the files on the USB device.

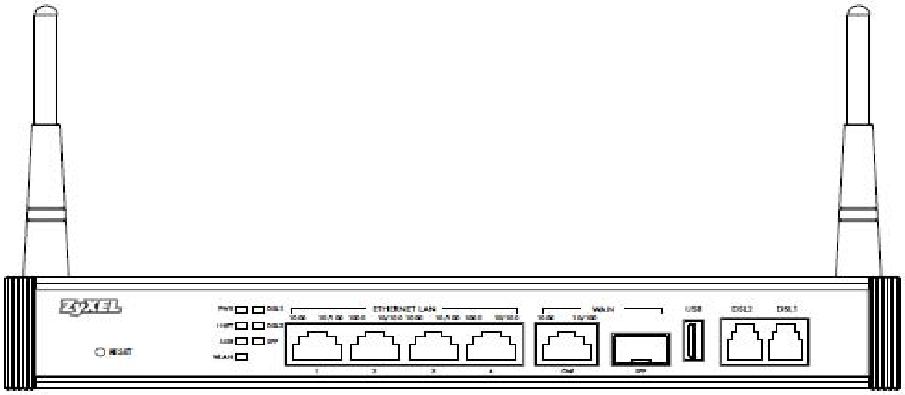
Figure 4 USB File Sharing Application



1.3 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 5 LEDs on the Device



None of the LEDs are on if the SBG3500-N is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The SBG3500-N is receiving power and ready for use.
		Blinking	The SBG3500-N is self-testing.
		Off	The SBG3500-N is not receiving power.
	Red	On	The SBG3500-N detected an error while self-testing, or there is a device malfunction.
		Off	The SBG3500-N is not receiving power.
ETHERNET LAN 1-4	Left LED (1000) Green	On	The SBG3500-N has a successful Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The SBG3500-N is sending or receiving data to/from the LAN.
		Off	The SBG3500-N does not have an Ethernet connection with the LAN.
	Right LED (10/100) Orange	On	The SBG3500-N has a successful Ethernet connection with a device on the Local Area Network (LAN).
		Blingking	The SBG3500-N is sending or receiving data to/from the LAN.
		Off	The SBG3500-N does not have an Ethernet connection with the LAN.
ETHERNET WAN	Left LED (1000) Green	On	The Gigabit Ethernet connection is working.
		Blinking	The SBG3500-N is sending or receiving data to/from the Gigabit Ethernet link.
		Off	There is no Gigabit Ethernet link.
	Right LED (10/100) Orange	On	The Gigabit Ethernet connection is working.
		Blinking	The SBG3500-N is sending or receiving data to/from the Gigabit Ethernet link.
		Off	There is no Gigabit Ethernet link.

Table 1 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
DSL1 and DSL2	Green	On	The ADSL2+ line is up.
		Blinking	The SBG3500-N is initializing the ADSL2+ line.
		Off	The ADSL2+ line is down.
	Orange	On	The VDSL line is up.
		Blinking	The SBG3500-N is initializing the VDSL line.
		Off	The VDSL line is down.
SFP	Green	On	The Fiber connection is working.
		Blinking	The SBG3500-N is sending or receiving data to/from the Fiber link.
		Off	There is no Fiber link.
INTERNET	Green	On	The SBG3500-N has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The SBG3500-N is sending or receiving IP or 3G traffic.
		Off	There is no Internet connection or the gateway is in bridged mode.
	Red	On	The SBG3500-N failed to establish an IP connection. No WAN IP address (either static or assigned by a DHCP server), PPPoE negotiation failed (if used) and there’s no DSL connection.
USB	Green	On	The SBG3500-N recognizes a 3G/USB connection.
		Blinking	The SBG3500-N is sending/receiving data to /from the USB device connected to it.
		Off	The SBG3500-N does not detect a USB connection.
WLAN	Green	On	The wireless network is activated.
		Blinking	The SBG3500-N is communicating with other wireless clients and is setting up a WPS connection.
		Off	The wireless network is not activated.

1.4 Ways to Manage the SBG3500-N

Use any of the following methods to manage the SBG3500-N.

- Web Configurator. This is recommended for everyday management of the SBG3500-N using a (supported) web browser.
- TR-069. This is an auto-configuration server used to remotely configure your SBG3500-N.

1.5 Good Habits for Managing the SBG3500-N

Do the following things regularly to make the SBG3500-N more secure and to manage the SBG3500-N more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters. The password must have at least six characters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the SBG3500-N to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the SBG3500-N. You could simply restore your last configuration.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the front of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

1. Make sure the **POWER** LED is on (not blinking).
2. To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

CHAPTER 2

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management of the SBG3500-N via Internet browser. Use Internet Explorer 11.0 and later versions with JavaScript enabled, or Mozilla Firefox 21 and later versions or Safari 6.0 and later versions or Google Chrome 26 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See Appendix C on page 364 if you need to make sure these functions are allowed in Internet Explorer.

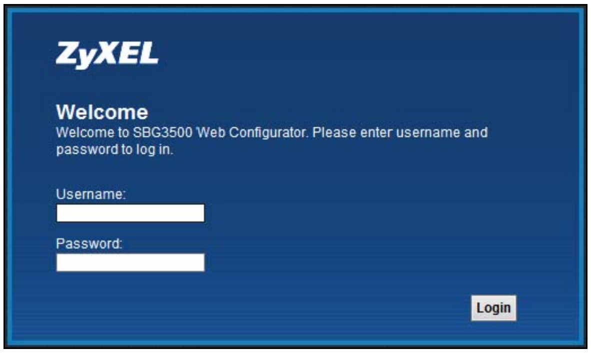
2.1.1 Accessing the Web Configurator

1 Make sure your SBG3500-N hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser. If the SBG3500-N does not automatically re-direct you to the login screen, go to http://192.168.1.1.

3 A password screen displays. To access the administrative web configurator and manage the SBG3500-N, type the default username **admin** and password **1234** in the password screen and click **Login**. If advanced account security is enabled (see Section 29.2 on page 300) the number of dots that appears when you type the password changes randomly to prevent anyone watching the password field from knowing the length of your password. If you have changed the password, enter your password and click **Login**.

Figure 6 Password Screen



ZyXEL

Welcome

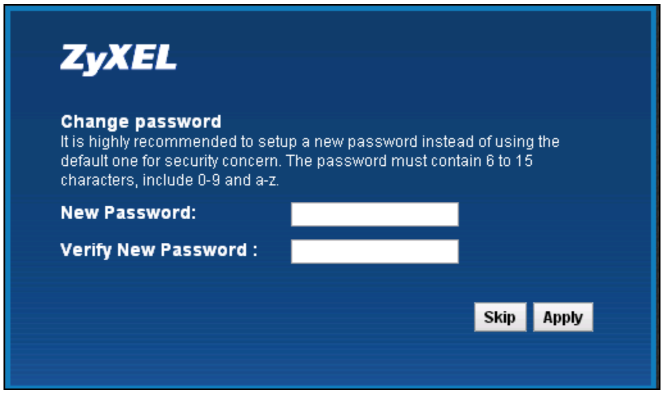
Welcome to SBG3500 Web Configurator. Please enter username and password to log in.

Username:

Password:

4 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, minding the rules in the screen, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

Figure 7 Change Password Screen



Change password

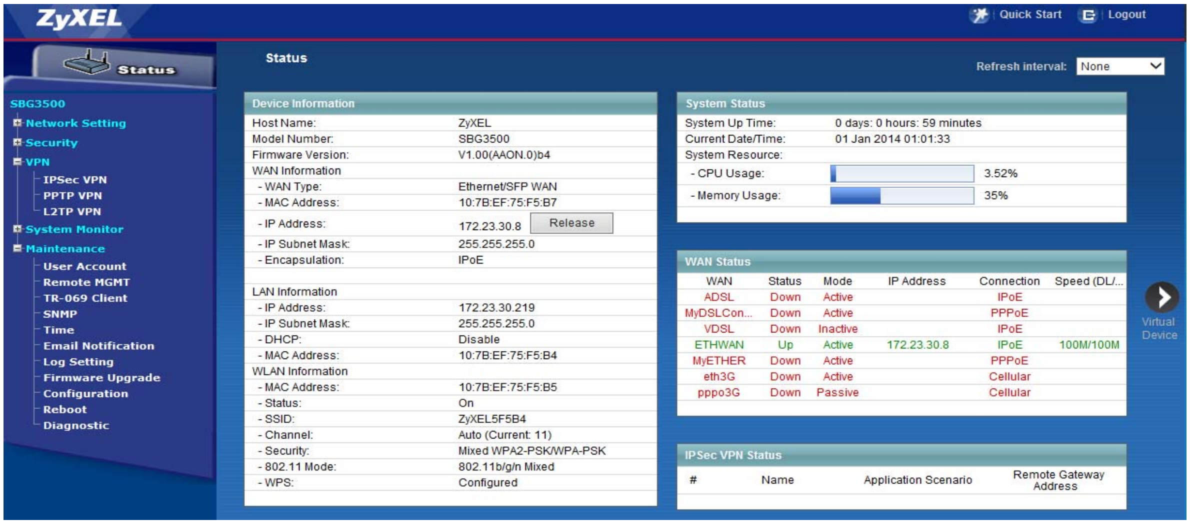
It is highly recommended to setup a new password instead of using the default one for security concern. The password must contain 6 to 15 characters, include 0-9 and a-z.

New Password:	
Verify New Password :	

5 The **Status** page appears, where you can view the SBG3500-N’s interface and system information.

6 Click the **Quick Start Wizard** button on top of the page to configure the SBG3500-N’s time zone, basic Internet access, and wireless settings. See Chapter 3 on page 32 for more information.

Figure 8 Status



Status

Refresh interval: None

Device Information	
Host Name:	ZyXEL
Model Number:	SBG3500
Firmware Version:	V1.00(AAON.0)b4
WAN Information	
- WAN Type:	Ethernet/SFP WAN
- MAC Address:	10:7B:EF:75:F5:B7
- IP Address:	172.23.30.8
- IP Subnet Mask:	255.255.255.0
- Encapsulation:	IPoE
LAN Information	
- IP Address:	172.23.30.219
- IP Subnet Mask:	255.255.255.0
- DHCP:	Disable
- MAC Address:	10:7B:EF:75:F5:B4
WLAN Information	
- MAC Address:	10:7B:EF:75:F5:B5
- Status:	On
- SSID:	ZyXEL5F5B4
- Channel:	Auto (Current: 11)
- Security:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured

System Status	
System Up Time:	0 days: 0 hours: 59 minutes
Current Date/Time:	01 Jan 2014 01:01:33
System Resource:	
- CPU Usage:	3.52%
- Memory Usage:	35%

WAN Status

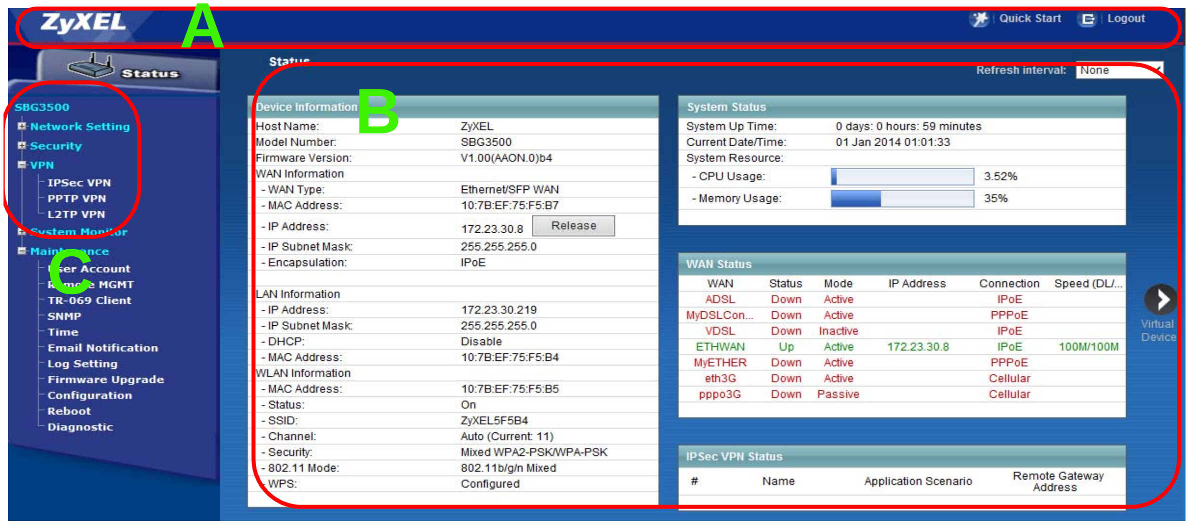
WAN	Status	Mode	IP Address	Connection	Speed (DL/...
ADSL	Down	Active		IPoE	
MyDSLCon...	Down	Active		PPPoE	
VDSL	Down	Inactive		IPoE	
ETHWAN	Up	Active	172.23.30.8	IPoE	100M/100M
MyETHER	Down	Active		PPPoE	
eth3G	Down	Active		Cellular	
pppo3G	Down	Passive		Cellular	

IPSec VPN Status

#	Name	Application Scenario	Remote Gateway Address

2.2 Web Configurator Layout

Figure 9 Screen Layout



Status

Refresh interval: None

Device Information

Host Name:	ZyXEL
Model Number:	SBG3500
Firmware Version:	V1.00(AAON.0)b4
WAN Information	
- WAN Type:	Ethernet/SFP WAN
- MAC Address:	10:7B:EF:75:F5:B7
- IP Address:	172.23.30.8
- IP Subnet Mask:	255.255.255.0
- Encapsulation:	IPoE
LAN Information	
- IP Address:	172.23.30.219
- IP Subnet Mask:	255.255.255.0
- DHCP:	Disable
- MAC Address:	10:7B:EF:75:F5:B4
WLAN Information	
- MAC Address:	10:7B:EF:75:F5:B5
- Status:	On
- SSID:	ZyXEL5F5B4
- Channel:	Auto (Current: 11)
- Security:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured

System Status

System Up Time:	0 days: 0 hours: 59 minutes
Current Date/Time:	01 Jan 2014 01:01:33
System Resource:	
- CPU Usage:	3.52%
- Memory Usage:	35%

WAN Status

WAN	Status	Mode	IP Address	Connection	Speed (DL/...
ADSL	Down	Active		IPoE	
MyDSLCon...	Down	Active		PPPoE	
VDSL	Down	Inactive		IPoE	
ETHWAN	Up	Active	172.23.30.8	IPoE	100M/100M
MyETHER	Down	Active		PPPoE	
eth3G	Down	Active		Cellular	
pppo3G	Down	Passive		Cellular	

IPSec VPN Status

#	Name	Application Scenario	Remote Gateway Address

As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

2.2.1 Title Bar

The title bar provides some icons in the upper right corner.

The icons provide the following functions.

Table 2 Web Configurator Icons in the Title Bar

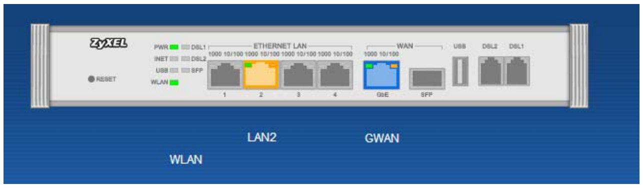
ICON	DESCRIPTION
Quick Start	**Quick Start**: Click this icon to open screens where you can configure the SBG3500-N's time zone Internet access, and wireless settings.
Logout	**Logout**: Click this icon to log out of the web configurator.

2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document. See Chapter 5 on page 99 for more information about the **Status** screen.

If you click **Virtual Device** on the **System Info** screen, a graphic shows the connection status of the Device’s ports. The connected interfaces are in color and disconnected interfaces are gray.

Figure 10 Virtual Device



2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure SBG3500-N features. The following tables describe each menu item.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		Click this to go to the main Web Configurator screen.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
	3G WAN	Use this screen to configure 3G WAN connection.
	Add New 3G Dongle	Use this screen to view or add a new 3G dongle.
	Advanced	Use this screen to enable or disable PTM over ADSL, Annex M, and DSL PhyR functions.
	802.1x	Use this screen to view and configure the IEEE 802.1x settings on the Device.
	Multi-WAN	Use this screen to configure the multiple WAN load balance and fail-over rules to distribute traffic among different interfaces.
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the SBG3500-N.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the SBG3500-N.
	WPS	Use this screen to configure and view your WPS (Wi-Fi Protected Setup) settings.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.
	Scheduling	Use this screen to set a schedule to turn off wireless LAN for power saving purposes.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
LAN	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	5th Ethernet Port	Use this screen to configure the Ethernet WAN port as a LAN port.
Routing	Static Route	Use this screen to view and set up static routes on the SBG3500-N.
	Policy Forwarding	Use this screen to configure policy routing on the SBG3500-N.
	RIP	Use this screen to set up RIP settings on the SBG3500-N.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Class Setup	Use this screen to define a classifier.
	Policer Setup	Use these screens to configure QoS policers.
	Monitor	Use this screen to view QoS packets statistics.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Applications	Use this screen to configure servers behind the SBG3500-N.
	Port Triggering	Use this screen to change your SBG3500-N’s port triggering settings.
	Default Server	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable or disable NAT ALG and SIP ALG.
	Address Mapping	Use this screen to change your Device’s address mapping settings.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Interface Group/VLAN	Interface Group/ VLAN	Use this screen to create a new interface group, which is a new LAN bridge interface (subnet).
USB Service	USB Service	Use this screen to enable file sharing via the SBG3500-N.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Service	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the SBG3500-N.
User Access Control	User Access Control	Use this screen to block web sites with the specific URL.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as User Access control) is enforced.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
VPN		
IPSec VPN	Setup	Use this screen to display and manage the SBG3500-N's IPSec VPN rules (tunnels).
	Monitor	Use this screen to display and manage active IPSec VPN connections.
	Radius	Use this screen to manage the list of RADIUS servers the SBG3500-N can use in authenticating users.
PPTP VPN	Setup	Use this screen to configure the PPTP VPN settings in the SBG3500-N.
	Monitor	Use this screen to view settings for PPTP clients.
L2TP VPN	Setup	Use this screen to configure the SBG3500-N's L2TP VPN settings.
	Monitor	Use this screen to view settings for L2TP clients.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the SBG3500-N. You can export or e-mail the logs.
	Security Log	Use this screen to view the login record of the SBG3500-N. You can export or e-mail the logs.
Network Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the SBG3500-N.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the SBG3500-N.
	DHCP Client	Use this screen to view the status of all wired and wireless devices connected to the SBG3500-N. You can also set screen refresh time to see updates on new devices.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table.
IGMP Group Status	IGMP Group Status	Use this screen to view the status of all IGMP settings on the SBG3500-N.
xDSL Statistics	xDSL Statistics	Use this screen to view the Device's xDSL traffic statistics.
Maintenance		
User Account	User Account	Use this screen to manage user accounts, which includes configuring the username, password, retry times, file sharing, captive portal, and customizing the login message.
Remote MGMT	Remote MGMT	Use this screen to enable specific traffic directions for network services.
TR-069 Client	TR-069 Clients	Use this screen to configure the SBG3500-N to be managed by an Auto Configuration Server (ACS).
SNMP	SNMP	Use this screen to enable/disable and configure settings for SNMP.
Time	Time	Use this screen to change your SBG3500-N's time and date.
Email Notification	Email Notification	Use this screen to configure up to two mail servers and sender addresses on the SBG3500-N.
Log Setting	Log Setting	Use this screen to change your SBG3500-N's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your device.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Configuration	Configuration	Use this screen to backup and restore your device’s configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the SBG3500-N without turning the power off.
Diagnostic	Ping & Traceroute & Nslookup	Use this screen to identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	OAM Ping	Use this screen to view information to help you identify problems with the DSL connection.

Quick Start

3.1 Overview

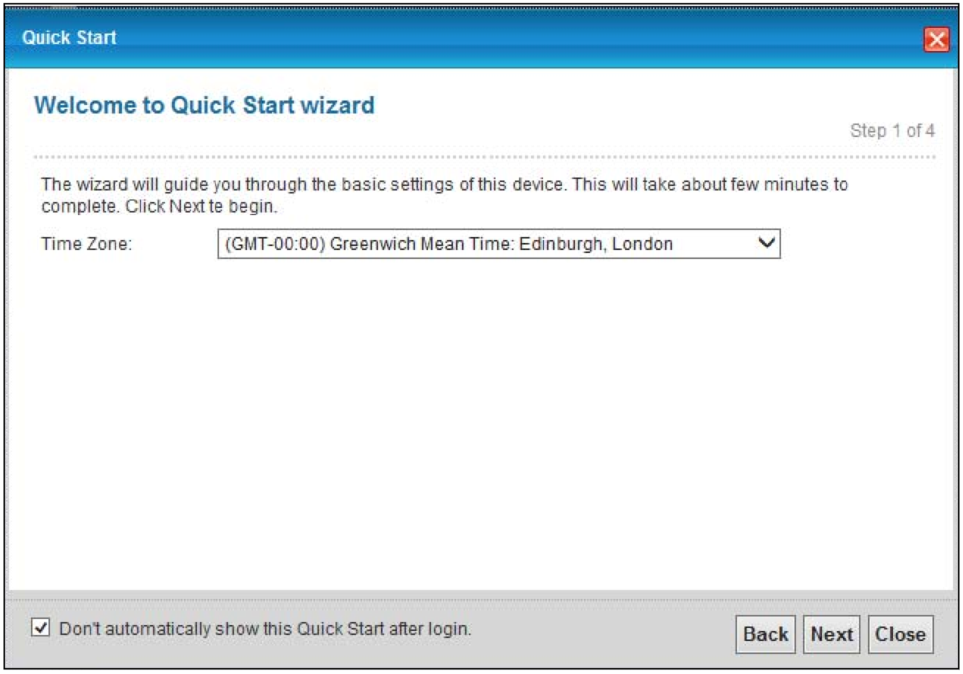
Use the **Quick Start** screens to configure the Device’s time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on page 97) for background information on the features in this chapter.

3.2 Quick Start Setup

1 The **Quick Start Wizard** appears automatically after login. Or you can click the **Click Start** icon in the top right corner of the web configurator to open the quick start screens. Select the time zone of the Device’s location and click **Next**.

Figure 11 Time Zone



Welcome to Quick Start wizard

Step 1 of 4

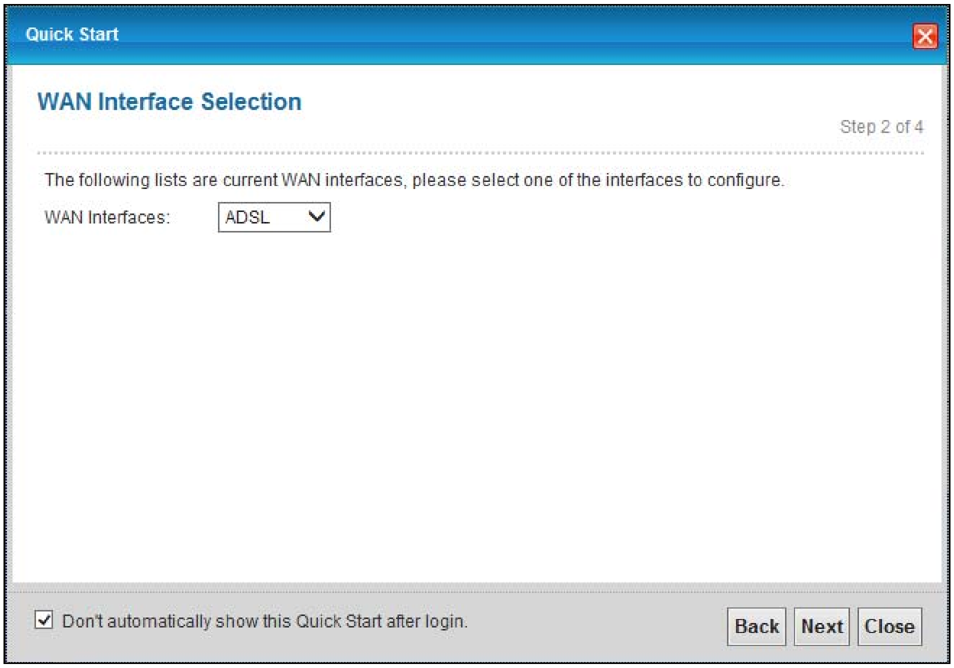
The wizard will guide you through the basic settings of this device. This will take about few minutes to complete. Click Next te begin.

Time Zone: (GMT-00:00) Greenwich Mean Time: Edinburgh, London

☑ Don't automatically show this Quick Start after login.

2 Select your current WAN interface to configure its settings.

Figure 12 WAN Interface Selection



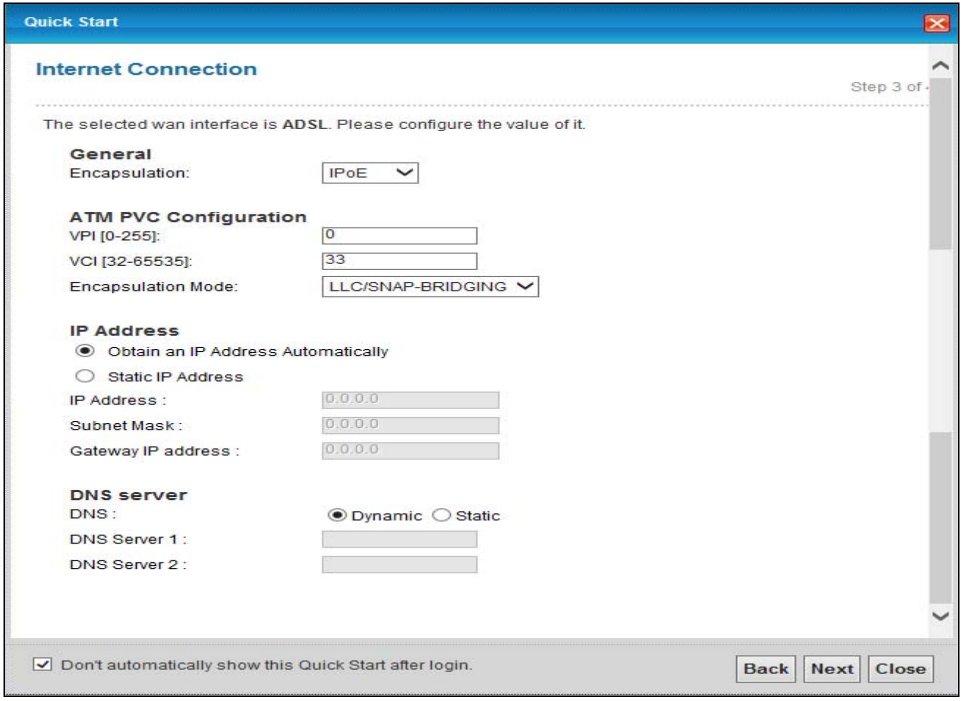
The following lists are current WAN interfaces, please select one of the interfaces to configure.

WAN Interfaces: ADSL

☑ Don't automatically show this Quick Start after login.

3 Enter your Internet connection information in this screen. The screen and fields to enter may vary depending on your current connection type. Click **Next**.

Figure 13 Internet Connection



The selected wan interface is **ADSL**. Please configure the value of it.

General

Encapsulation: IPoE

ATM PVC Configuration

VPI [0-255]: 0

VCI [32-65535]: 33

Encapsulation Mode: LLC/SNAP-BRIDGING

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway IP address : 0.0.0.0

DNS server

DNS : ● Dynamic ○ Static

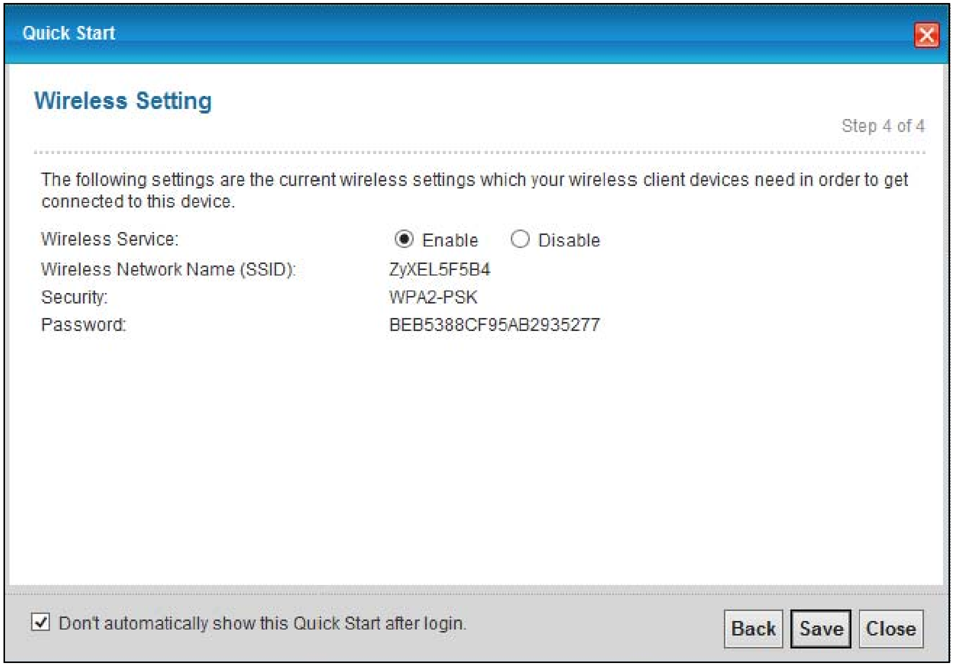
DNS Server 1 :

DNS Server 2 :

☑ Don't automatically show this Quick Start after login.

4 Turn the wireless LAN on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the Device. Click **Save**.

Figure 14 Internet Connection



Wireless Setting

Step 4 of 4

The following settings are the current wireless settings which your wireless client devices need in order to get connected to this device.

Wireless Service:	● Enable ○ Disable
Wireless Network Name (SSID):	ZyXEL5F5B4
Security:	WPA2-PSK
Password:	BEB5388CF95AB2935277

☑ Don't automatically show this Quick Start after login.

5 Your Device saves your settings and attempts to connect to the Internet.

4

Tutorials

4.1 Overview

This chapter shows you how to use the Device’s various features.

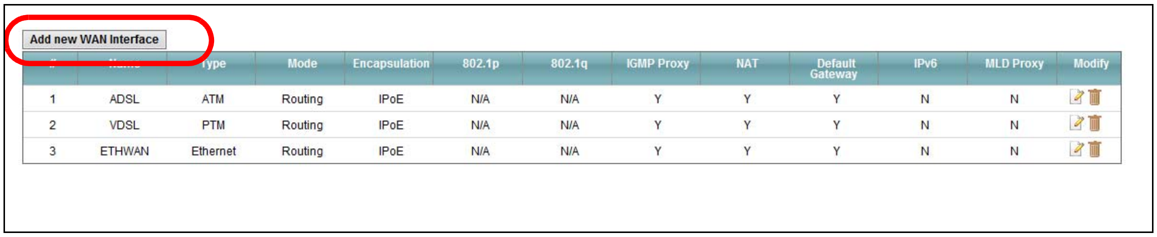
- Setting Up an ADSL PPPoE Connection, see page 35
- Setting Up a GbE WAN connection, see page 38
- Setting Up a 3G WAN connction, see page 40
- Setting Up a Secure Wireless Network, see page 41
- Setting Up Multiple Wireless Groups, see page 48
- Configuring Static Route for Routing to Another Network, see page 51
- Configuring QoS Queue and Class Setup, see page 54
- Access the Device Using DDNS, see page 57
- Configuring the MAC Address Filter, see page 59
- Access Your Shared Files From a Computer, see page 60
- Certificate Configuration for VPN, see page 61
- Examples of Configuring IPSec VPN Rules, see page 64
- PPTP VPN Tutorial, see page 69
- L2TP VPN Tutorial, see page 81

4.2 Setting Up an ADSL PPPoE Connection

This tutorial shows you how to set up your Internet connection using the Web Configurator.

If you connect to the Internet through an ADSL connection, use the information from your Internet Service Provider (ISP) to configure the Device. Be sure to contact your service provider for any information you need to configure the **Broadband** screens.

1 Click **Network Setting > Broadband** to open the following screen. Click **Add New WAN Interface**.



#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
2	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
3	ETHWAN	Ethernet	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑

2 In this example, the DSL connection has the following information.

General	
Name	MyDSLConnection
Type	ADSL
Connection Mode	Routing
Encapsulation	PPPoE
IPv6/IPv4 Mode	IPv4
ATM PVC Configuration	
VPI/VCI	36/48
Encapsulation Mode	LLC/SNAP-Bridging
Service Category	UBR without PCR
Account Information	
PPP User Name	1234@DSL-Ex.com
PPP Password	ABCDEF!
PPPoE Service Name	MyDSL
Static IP Address	192.168.1.32
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enabled

3 Select the **Active** check box. Enter the **General** and **ATM PVC Configuration** settings as provided above.

Set the **Type** to **ADSL over ATM**.

Choose the **Encapsulation** specified by your DSL service provider. For this example, the service provider requires a username and password to establish Internet connection. Therefore, select **PPPoE** as the WAN encapsulation type.

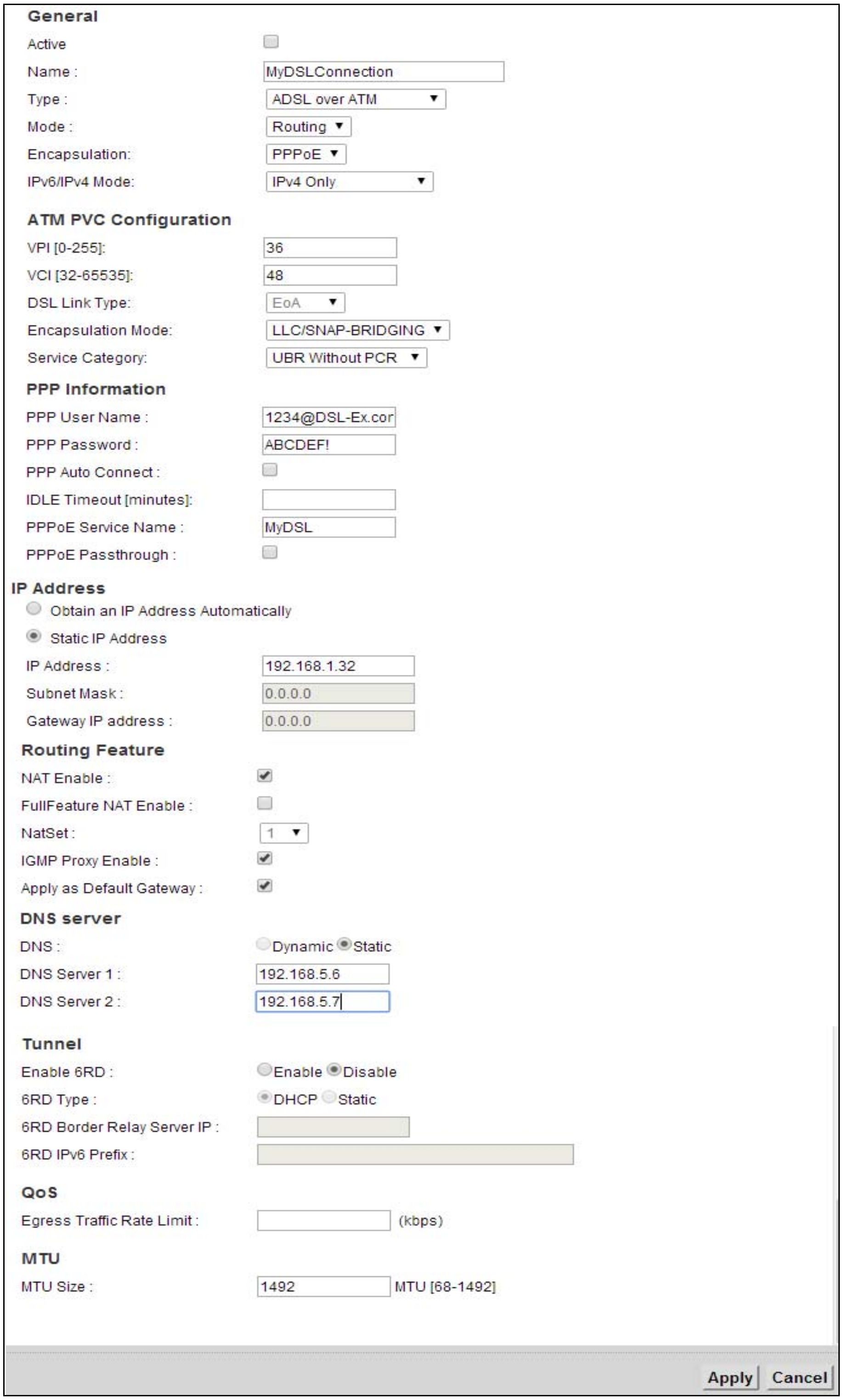
Set the **IPv6/IPv4 Mode** to **IPv4 Only**.

4 Enter the account information provided to you by your DSL service provider.

5 Configure this rule as your default Internet connection by selecting the **Apply as Default Gateway** check box. Then select DNS as **Static** and enter the DNS server addresses provided to you, such as **192.168.5.2** (DNS server1)/**192.168.5.1** (DNS server2).

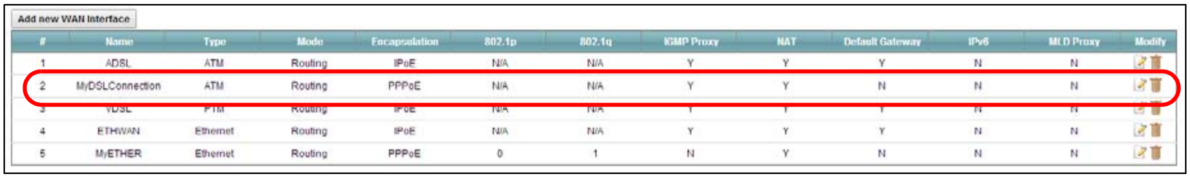
6 Leave the rest of the fields to the default settings.

7 Click **Apply** to save your settings.



General	
Active	☐
Name :	MyDSLConnection
Type :	ADSL over ATM ▼
Mode :	Routing ▼
Encapsulation:	PPPoE ▼
IPv6/IPv4 Mode:	IPv4 Only ▼
ATM PVC Configuration	
VPI [0-255]:	36
VCI [32-65535]:	48
DSL Link Type:	EoA ▼
Encapsulation Mode:	LLC/SNAP-BRIDGING ▼
Service Category:	UBR Without PCR ▼
PPP Information	
PPP User Name :	1234@DSL-Ex.cor
PPP Password :	ABCDEF!
PPP Auto Connect :	☐
IDLE Timeout [minutes]:	
PPPoE Service Name :	MyDSL
PPPoE Passthrough :	☐
IP Address	
○ Obtain an IP Address Automatically	
● Static IP Address	
IP Address :	192.168.1.32
Subnet Mask :	0.0.0.0
Gateway IP address :	0.0.0.0
Routing Feature	
NAT Enable :	☑
FullFeature NAT Enable :	☐
NatSet :	1 ▼
IGMP Proxy Enable :	☑
Apply as Default Gateway :	☑
DNS server	
DNS :	○ Dynamic ● Static
DNS Server 1 :	192.168.5.6
DNS Server 2 :	192.168.5.7
Tunnel	
Enable 6RD :	○ Enable ● Disable
6RD Type :	● DHCP ○ Static
6RD Border Relay Server IP :	
6RD IPv6 Prefix :	
QoS	
Egress Traffic Rate Limit :	(kbps)
MTU	
MTU Size :	1492 MTU [68-1492]

8 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows.



#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
2	MyDSLConnection	ATM	Routing	PPPoE	N/A	N/A	Y	Y	N	N	N	✎ 🗑
3	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
4	ETHWAN	Ethernet	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
5	MyETHER	Ethernet	Routing	PPPoE	0	1	N	Y	N	N	N	✎ 🗑

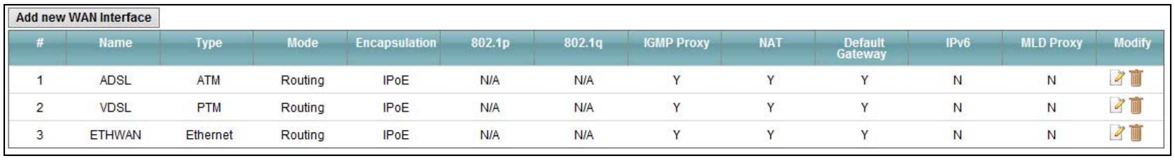
Try to connect to a website to see if you have correctly set up your Internet connection. Be sure to contact your service provider for any information you need to configure the WAN screens.

4.3 Setting Up a GbE WAN connection

This tutorial shows you how to set up your Gigabit Ethernet WAN connection using the Web Configurator.

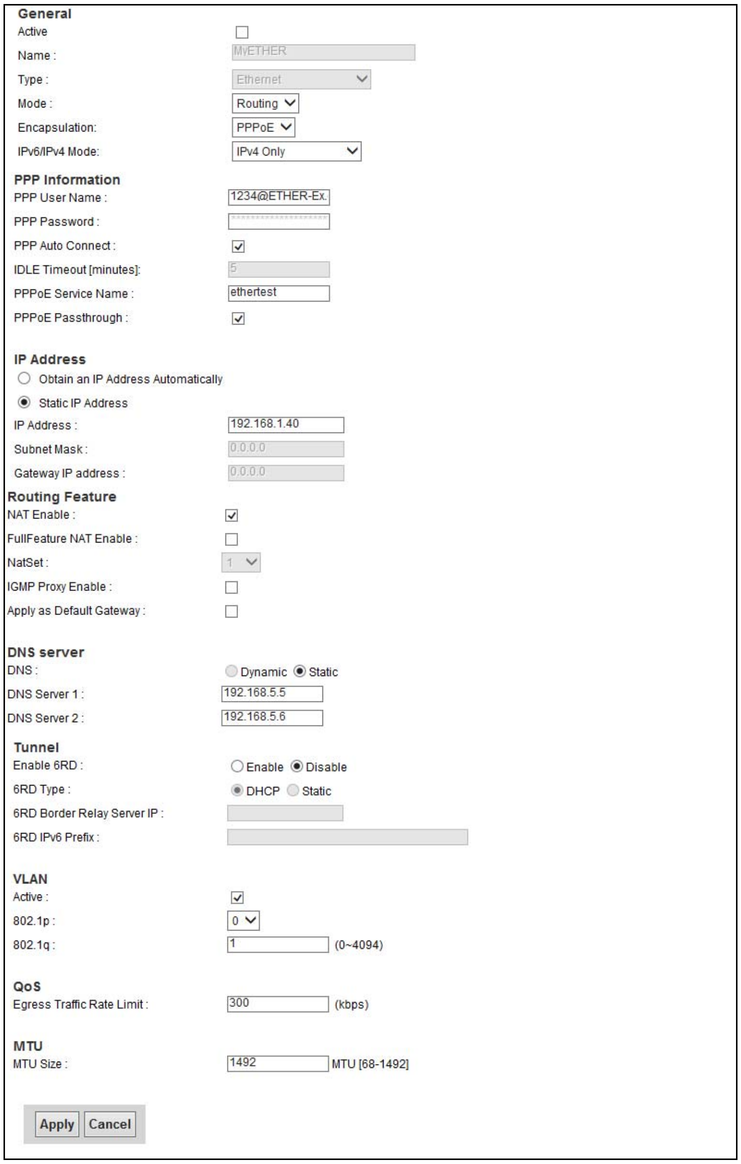
If you connect to the Internet through an Ethernet connection, use the information from your Internet Service Provider (ISP) to configure the Device. Be sure to contact your service provider for any information you need to configure the **Broadband** screens.

1 Click **Network Setting** > **Broadband** to open the following screen.



#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
2	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
3	ETHWAN	Ethernet	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑

2 Next, click **Add New WAN Interface** to open the following screen.



General

Active ☐

Name : MyETHER

Type : Ethernet

Mode : Routing

Encapsulation: PPPoE

IPv6/IPv4 Mode: IPv4 Only

PPP Information

PPP User Name : 1234@ETHER-Ex.

PPP Password : ********************

PPP Auto Connect : ☑

IDLE Timeout [minutes]: 5

PPPoE Service Name : ethertest

PPPoE Passthrough : ☑

IP Address

○ Obtain an IP Address Automatically

● Static IP Address

IP Address : 192.168.1.40

Subnet Mask : 0.0.0.0

Gateway IP address : 0.0.0.0

Routing Feature

NAT Enable : ☑

FullFeature NAT Enable : ☐

NatSet : 1

IGMP Proxy Enable : ☐

Apply as Default Gateway : ☐

DNS server

DNS : ○ Dynamic ● Static

DNS Server 1 : 192.168.5.5

DNS Server 2 : 192.168.5.6

Tunnel

Enable 6RD : ○ Enable ● Disable

6RD Type : ● DHCP ○ Static

6RD Border Relay Server IP :

6RD IPv6 Prefix :

VLAN

Active : ☑

802.1p : 0

802.1q : 1 (0~4094)

QoS

Egress Traffic Rate Limit : 300 (kbps)

MTU

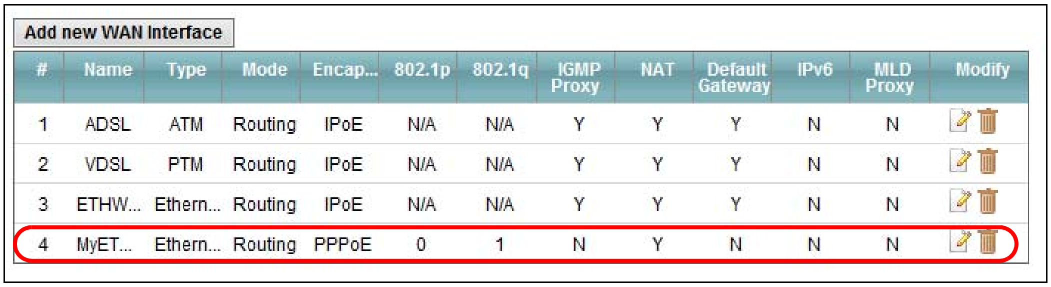
MTU Size : 1492 MTU [68-1492]

In this example, the Ethernet connection has the following information.

General	
Name	MyETHER
Type	Ethernet
Mode	Routing
Service and Encapsulation	PPPoE
IPv6/IPv4 Mode	IPv4
Account Information	
802.1p	0
802.1q	1
QoS	300 kbps

PPP User Name	1234@ETHER-Ex.com
PPP Password	ABCDEF!
PPP Auto Connect	Enabled
PPPoE Service name	ethertest
PPPoE Passthrough	Enabled
MTU	1492
IP Address	192.168.1.40
Primary DNS Server	192.168.5.5
Secondary DNS Server	192.168.5.6
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enabled

You should see a summary of your new Ethernet connection setup in the **Broadband** screen as follows.



Add new WAN Interface

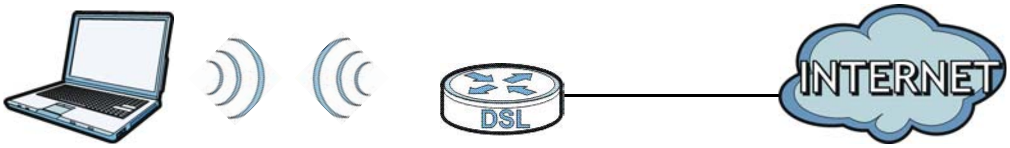
#	Name	Type	Mode	Encap...	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
2	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
3	ETHW...	Ethern...	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
4	MyET...	Ethern...	Routing	PPPoE	0	1	N	Y	N	N	N	✎ 🗑

4.4 Setting Up a 3G WAN connction

See the **3G WAN** screen (Section 6.3 on page 116) for setting up a 3G WAN connection. Make sure you insert a valid SIM card (with active data plan) into the 3G USB dongle before you inser the USB dongle to the USB port of your computer.

4.5 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



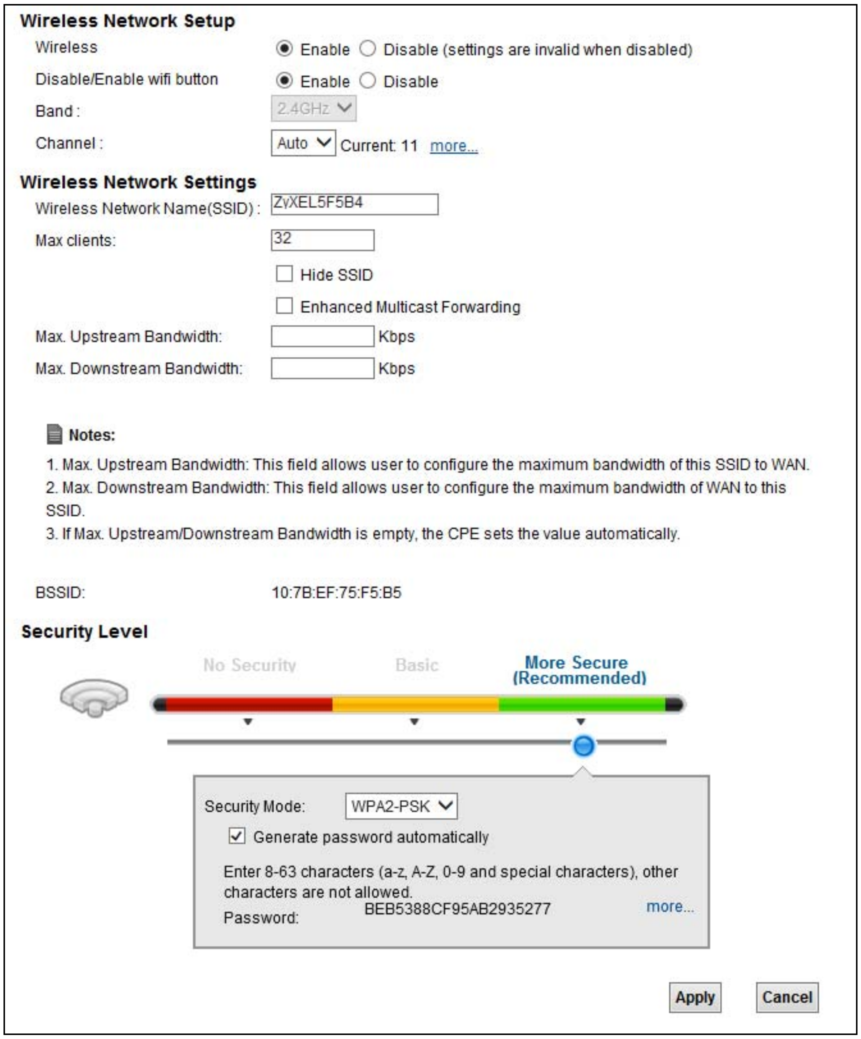
Thomas has to configure the wireless network settings on the Device. Then he can set up a wireless network using WPS (Section 4.5.2 on page 43) or manual configuration (Section 4.5.3 on page 47).

4.5.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network.

SSID	Example
Security Mode	WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n Mixed

1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see page 41). Click **Apply**.



Wireless Network Setup

Wireless ● Enable ○ Disable (settings are invalid when disabled)

Disable/Enable wifi button ● Enable ○ Disable

Band : 2.4GHz

Channel : Auto Current: 11 more...

Wireless Network Settings

Wireless Network Name(SSID) : ZyXEL5F5B4

Max clients: 32

□ Hide SSID

□ Enhanced Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

BSSID: 10:7B:EF:75:F5:B5

Security Level

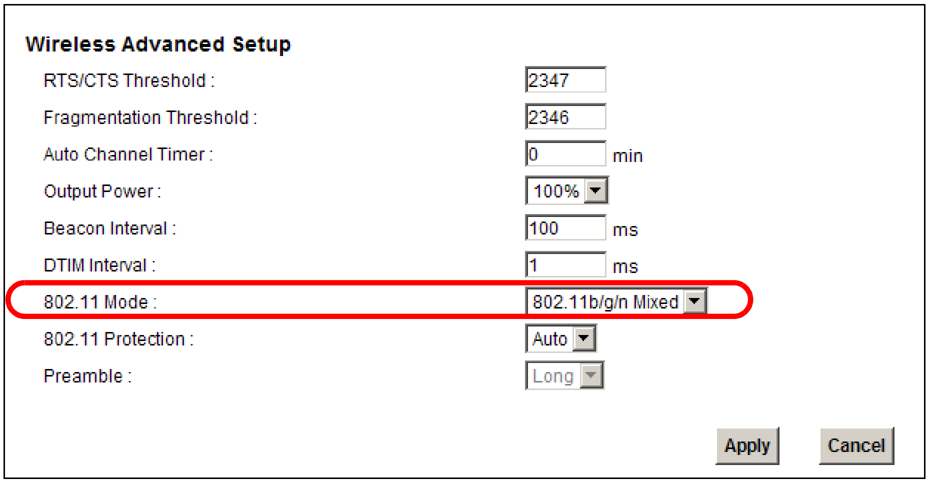
Security Mode: WPA2-PSK

☑ Generate password automatically

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

Password: BEB5388CF95AB2935277 more...

2 Go to the **Wireless > Others** screen and select **802.11b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.



Wireless Advanced Setup

RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346
Auto Channel Timer :	0 min
Output Power :	100%
Beacon Interval :	100 ms
DTIM Interval :	1 ms
802.11 Mode :	802.11b/g/n Mixed
802.11 Protection :	Auto
Preamble :	Long

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the Device (see Section 4.5.2 on page 43). He can also use the notebook's wireless client to search for the Device (see Section 4.5.3 on page 47).

4.5.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the Device as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card).

There are two WPS methods to set up the wireless client settings:

- **Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **PIN Configuration** - configure a Personal Identification Number (PIN) on the Device. A wireless client must also use the same PIN in order to download the wireless network settings from the Device.

Push Button Configuration (PBC)

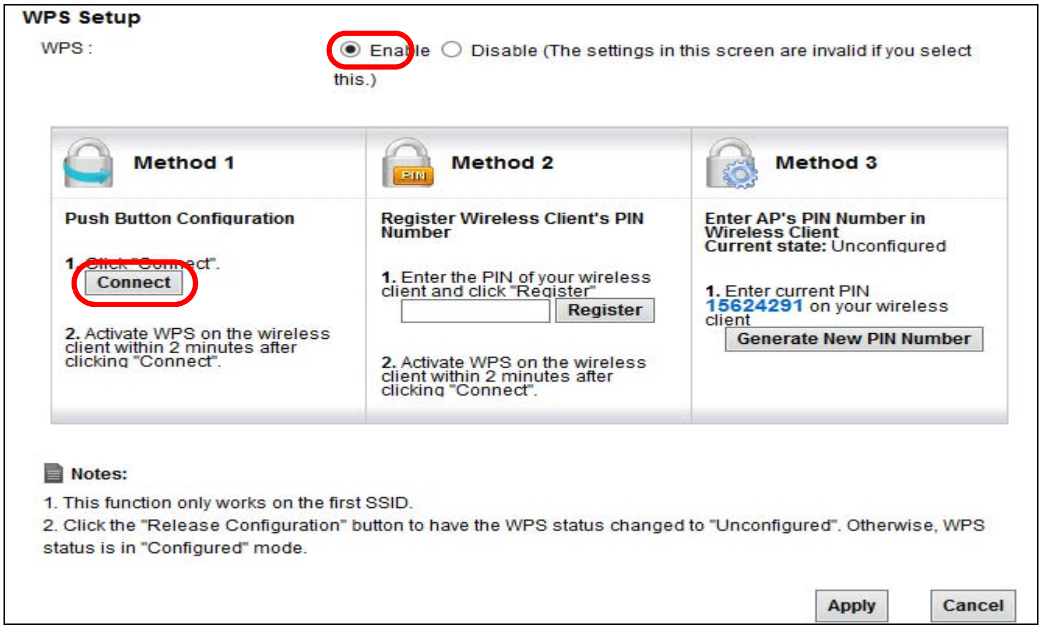
1 Make sure that your Device is turned on and your notebook is within the cover range of the wireless signal.

2 Make sure that you have installed the wireless client driver and utility in your notebook.

3 In the wireless client utility, go to the WPS setting page. Enable WPS and press the WPS button (**Start** or **WPS** button).

4 Log into Device's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**. Then click the **Connect** button.

Note: You must enable the **Wireless** function in the **Network Setting** > **Wireless** > **General** screen before you can enable the WPS function.



WPS Setup

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

Method 1

Push Button Configuration

1. Click "Connect".

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click "Register"

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

Enter AP's PIN Number in Wireless Client

Current state: Unconfigured

1. Enter current PIN **15624291** on your wireless client

Notes:

1. This function only works on the first SSID.

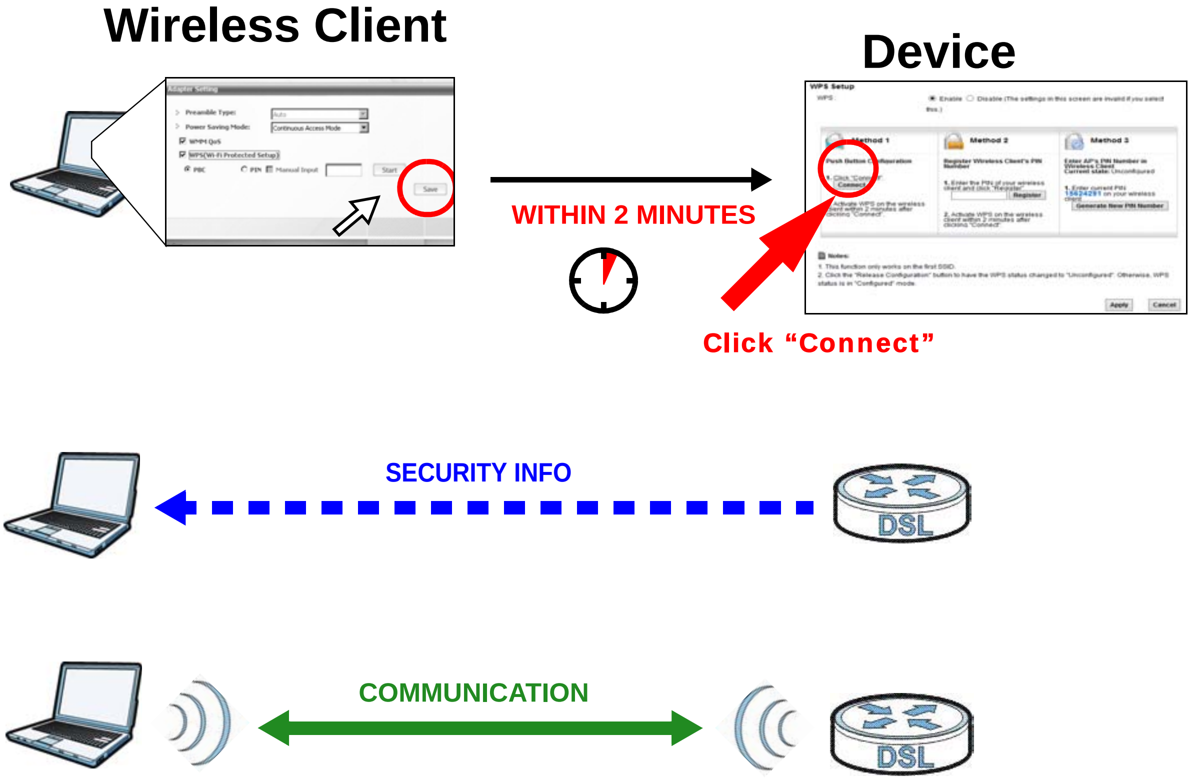
2. Click the "Release Configuration" button to have the WPS status changed to "Unconfigured". Otherwise, WPS status is in "Configured" mode.

Note: Your Device has a WPS button located on its front panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn't matter which device's WPS you enable first, but you must enable the second device's WPS within two minutes of enabling the first one.

The Device sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Device securely.

The following figure shows you an example of how to set up a wireless network and its security.

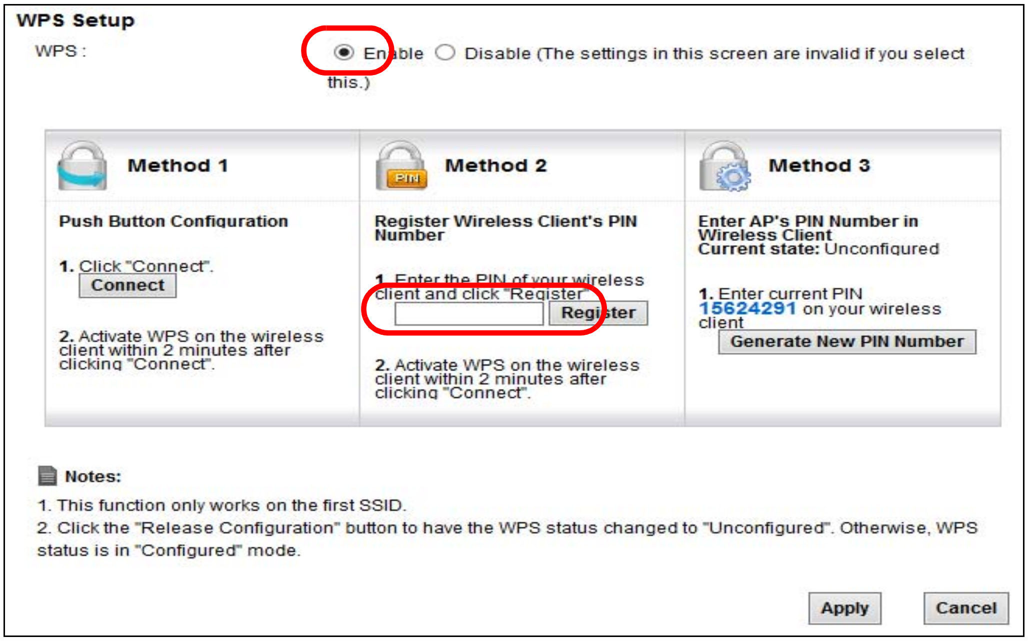


PIN Configuration

When you use the PIN configuration method, you need to use both the Device's web configurator and the wireless client's utility.

1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

2 Log into Device's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**.



WPS Setup

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

Method 1	**Method 2**	**Method 3**
Push Button Configuration	**Register Wireless Client's PIN Number**	**Enter AP's PIN Number in Wireless Client** **Current state:** Unconfigured
1. Click "Connect". Connect	**1.** Enter the PIN of your wireless client and click "Register" Register	**1.** Enter current PIN **15624291** on your wireless client Generate New PIN Number
2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".	**2.** Activate WPS on the wireless client within 2 minutes after clicking "Connect".	

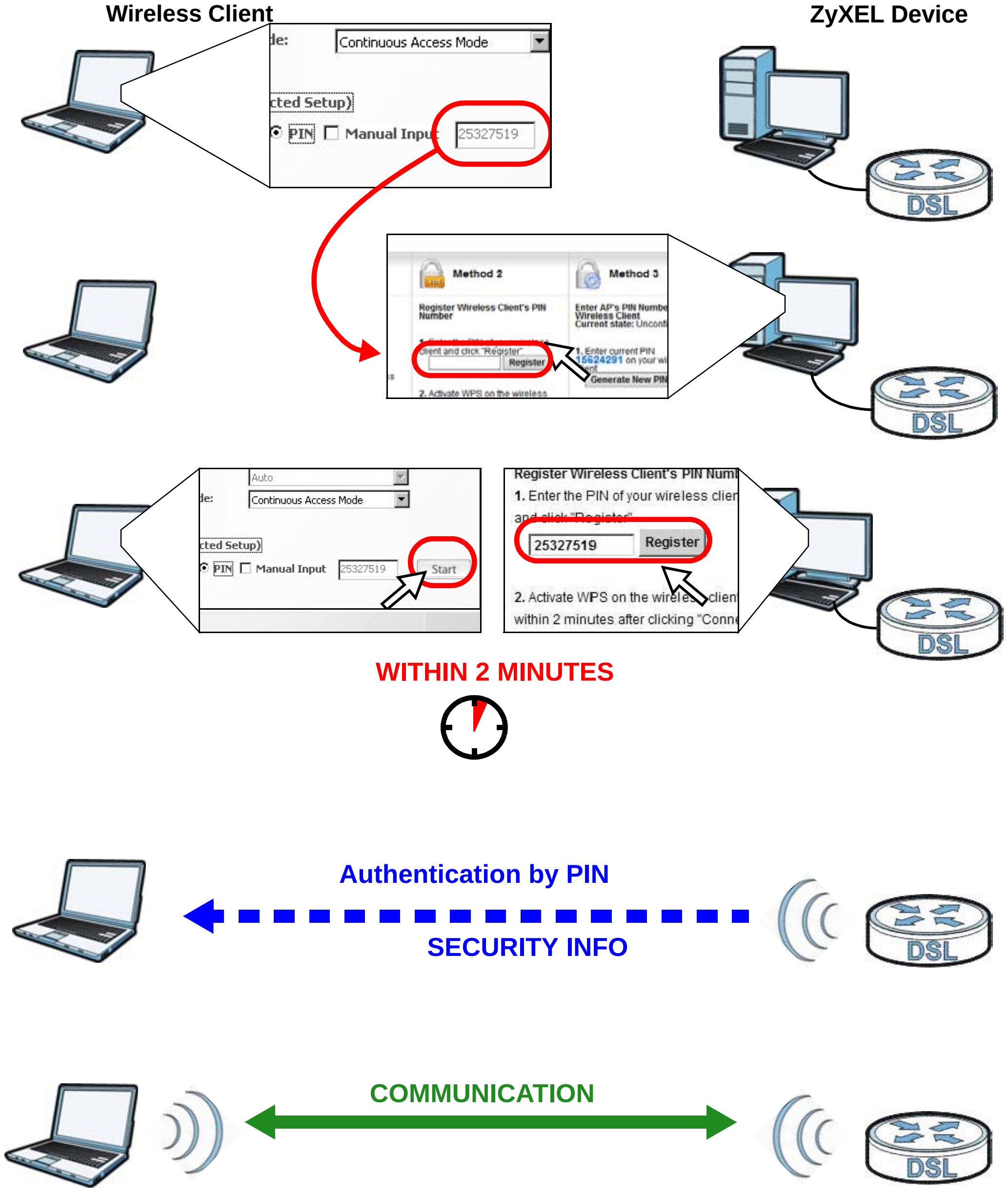
Notes:

1. This function only works on the first SSID.
2. Click the "Release Configuration" button to have the WPS status changed to "Unconfigured". Otherwise, WPS status is in "Configured" mode.

3 Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.

The Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Device securely.

The following figure shows you how to set up a wireless network and its security on a Device and a wireless client by using PIN method.



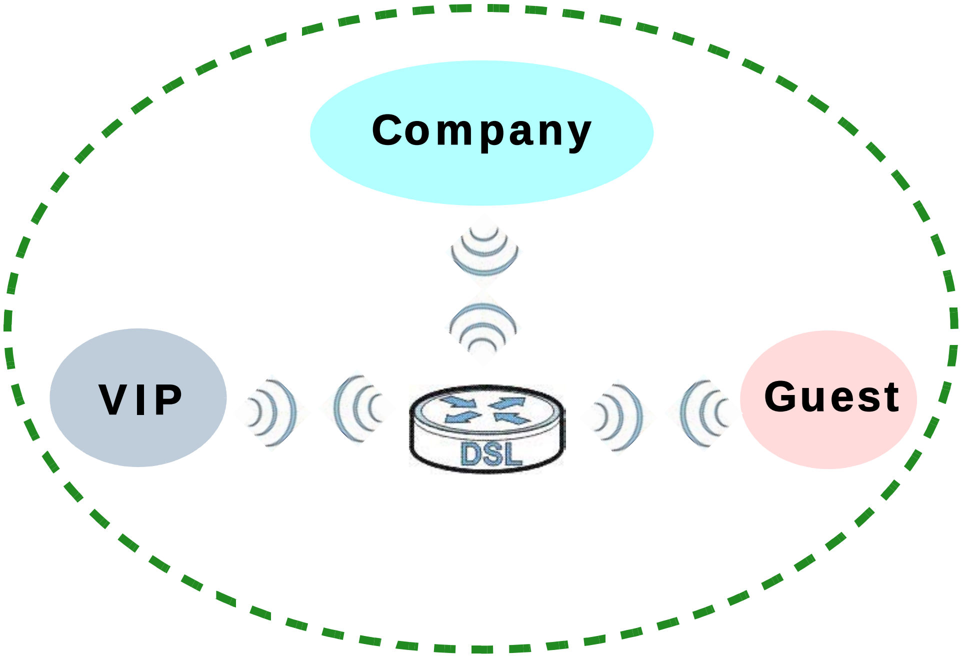
4.5.3 Without WPS

Use the wireless adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish an wireless Internet connection.

Note: The Device supports IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

4.6 Setting Up Multiple Wireless Groups

Company A wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own SSID and security mode.

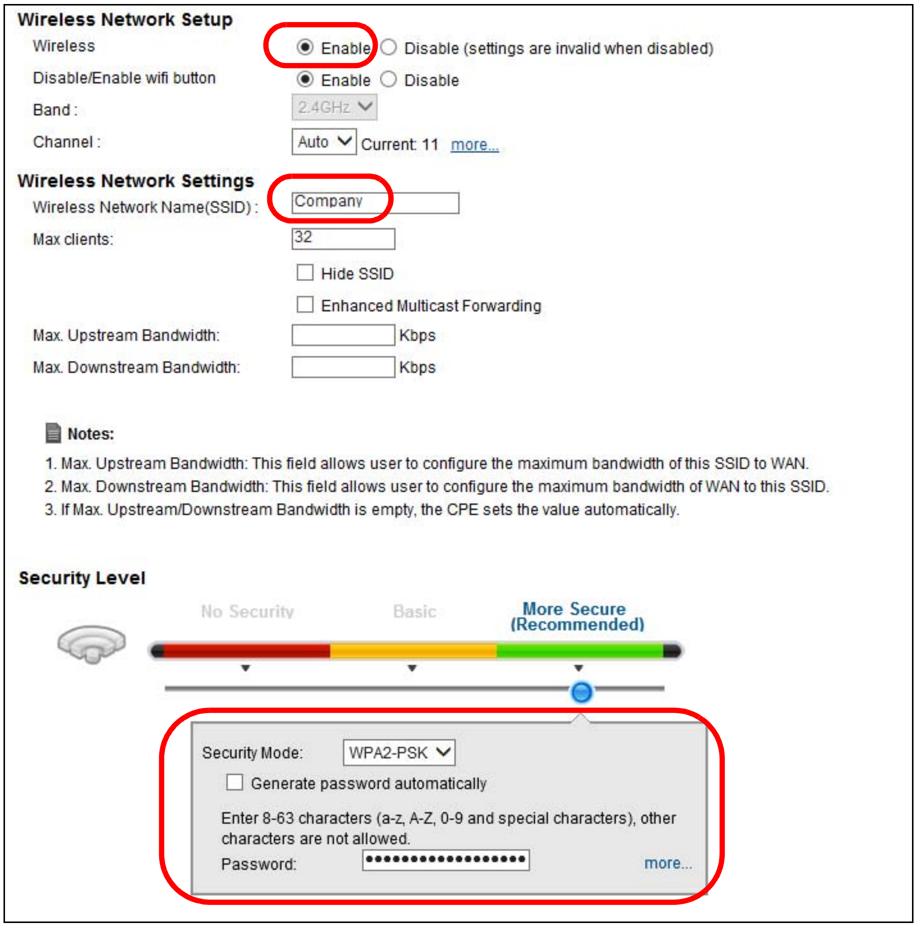


- Employees in Company A will use a general **Company** wireless network group.
- Higher management level and important visitors will use the **VIP** group.
- Visiting guests will use the **Guest** group, which has a lower security mode.

Company A will use the following parameters to set up the wireless network groups.

	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	Basic
Security Mode	WPA2-PSK	WPA2-PSK	Static WEP
Pre-Shared Key	ForCompanyOnly	ForVIPOnly	Guest12345678

1 Click **Network Setting > Wireless** to open the **General** screen. Use this screen to set up the company's general wireless network group. Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

Wireless ● Enable ○ Disable (settings are invalid when disabled)

Disable/Enable wifi button ● Enable ○ Disable

Band : 2.4GHz

Channel : Auto Current: 11 more...

Wireless Network Settings

Wireless Network Name(SSID) : Company

Max clients: 32

□ Hide SSID

□ Enhanced Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

Security Level

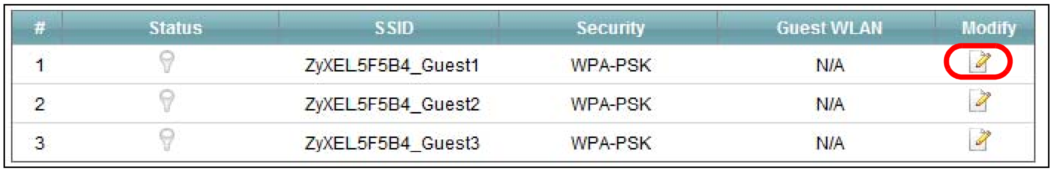
Security Mode: WPA2-PSK

□ Generate password automatically

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

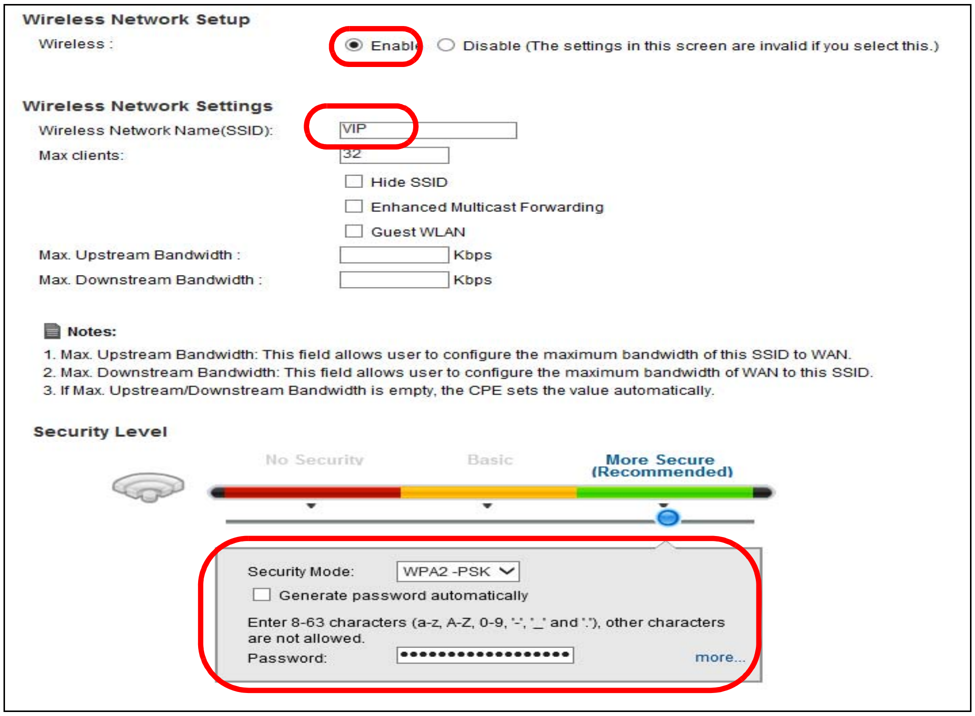
Password: ••••••••••••••••••• more...

2 Click **Network Setting > Wireless > More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.



#	Status	SSID	Security	Guest WLAN	Modify
1		ZyXEL5F5B4_Guest1	WPA-PSK	N/A	✎
2		ZyXEL5F5B4_Guest2	WPA-PSK	N/A	✎
3		ZyXEL5F5B4_Guest3	WPA-PSK	N/A	✎

3 Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

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

Wireless Network Settings

Wireless Network Name(SSID): VIP

Max clients: 32

□ Hide SSID

□ Enhanced Multicast Forwarding

□ Guest WLAN

Max. Upstream Bandwidth : Kbps

Max. Downstream Bandwidth : Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

Security Level

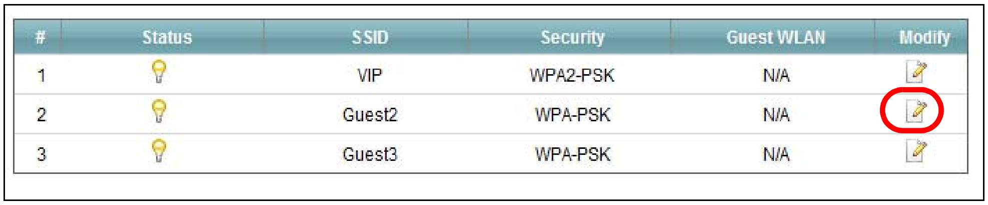
Security Mode: WPA2 -PSK

□ Generate password automatically

Enter 8-63 characters (a-z, A-Z, 0-9, '-', '_' and '.'), other characters are not allowed.

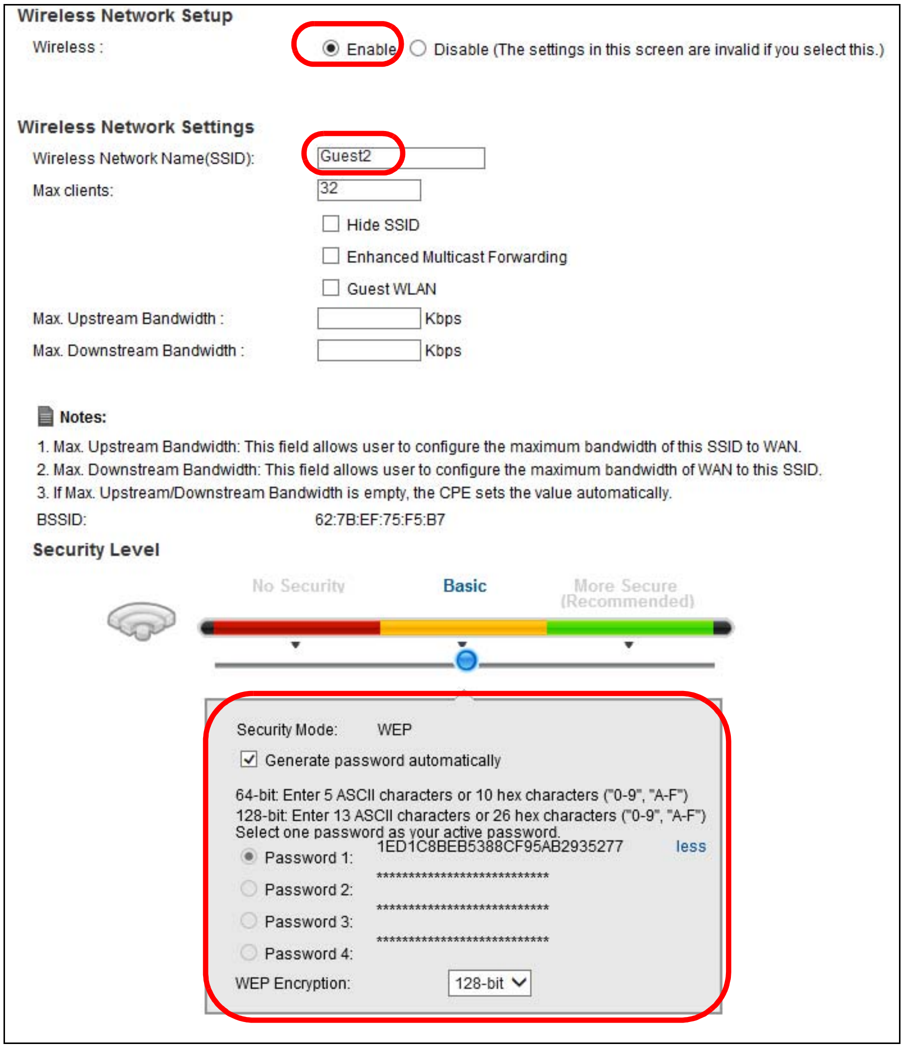
Password: •••••••••••••••••••

4 In the **More AP** screen, click the **Edit** icon to configure the third wireless network group.



#	Status	SSID	Security	Guest WLAN	Modify
1	💡	VIP	WPA2-PSK	N/A	✎
2	💡	Guest2	WPA-PSK	N/A	✎
3	💡	Guest3	WPA-PSK	N/A	✎

5 Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

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

Wireless Network Settings

Wireless Network Name(SSID): Guest2

Max clients: 32

□ Hide SSID

□ Enhanced Multicast Forwarding

□ Guest WLAN

Max. Upstream Bandwidth : Kbps

Max. Downstream Bandwidth : Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

BSSID: 62:7B:EF:75:F5:B7

Security Level

Security Mode: WEP

☑ Generate password automatically

64-bit: Enter 5 ASCII characters or 10 hex characters ("0-9", "A-F")
128-bit: Enter 13 ASCII characters or 26 hex characters ("0-9", "A-F")
Select one password as your active password.

● Password 1: 1ED1C8BEB5388CF95AB2935277 less

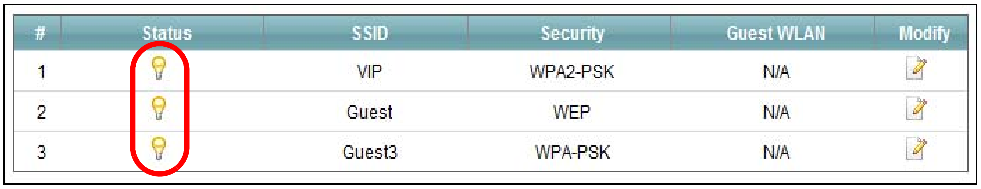
○ Password 2: **************************

○ Password 3: **************************

○ Password 4: **************************

WEP Encryption: 128-bit

6 Check the status of **VIP** and **Guest** in the **More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

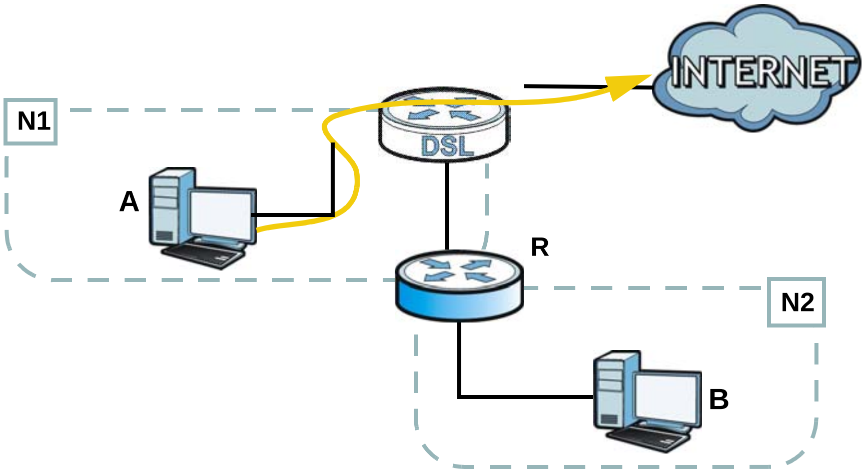


#	Status	SSID	Security	Guest WLAN	Modify
1	💡	VIP	WPA2-PSK	N/A	✎
2	💡	Guest	WEP	N/A	✎
3	💡	Guest3	WPA-PSK	N/A	✎

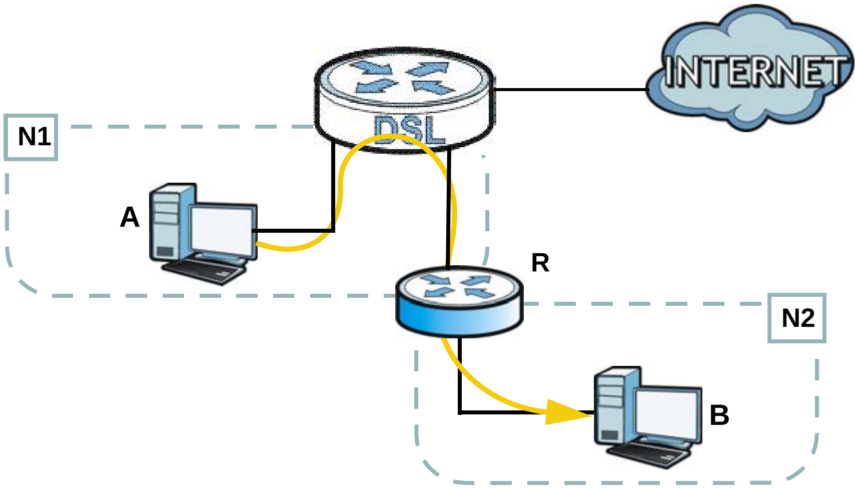
4.7 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 4 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Device's WAN	172.16.1.1
The Device's LAN	192.168.1.1
IP Type	IPv4
Use Interface	ADSL/atm0
A	192.168.1.34

Table 4 IP Settings in this Tutorial

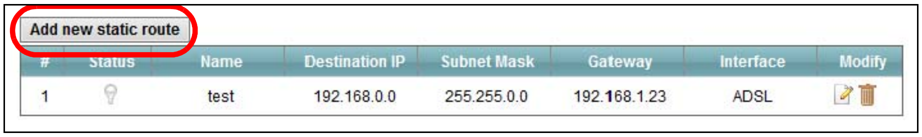
DEVICE / COMPUTER	IP ADDRESS
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Log into the Device's Web Configurator in advanced mode.

2 Click **Network Setting** > **Routing**.

3 Click **Add new static route** in the **Static Route** screen.



Add new static route

#	Status	Name	Destination IP	Subnet Mask	Gateway	Interface	Modify
1		test	192.168.0.0	255.255.0.0	192.168.1.23	ADSL	

4 Configure the **Static Route Setup** screen using the following settings:

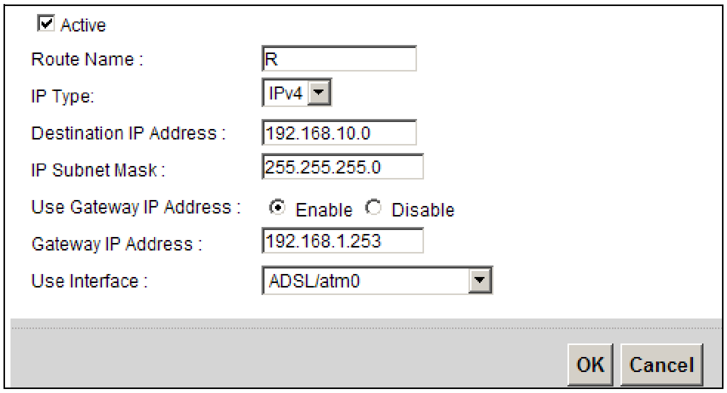
4a Select the **Active** check box. Enter the **Route Name** as **R**.

4b Set **IP Type** to **IPv4**.

4c Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

4d Select **Enable** in the **Use Gateway IP Address field**. Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.

4e Select **ADSL/atm0** as the **Use Interface**.



☑ Active

Route Name :	R
IP Type:	IPv4
Destination IP Address :	192.168.10.0
IP Subnet Mask :	255.255.255.0
Use Gateway IP Address :	● Enable ○ Disable
Gateway IP Address :	192.168.1.253
Use Interface :	ADSL/atm0

OK Cancel

4a Click **OK**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

4.8 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

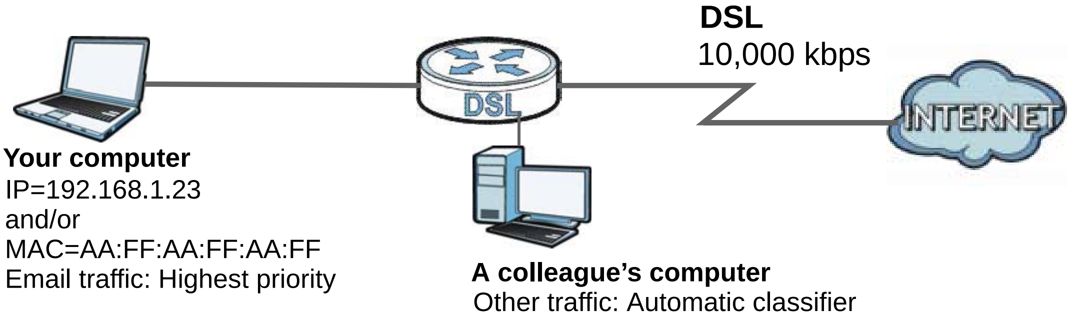
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

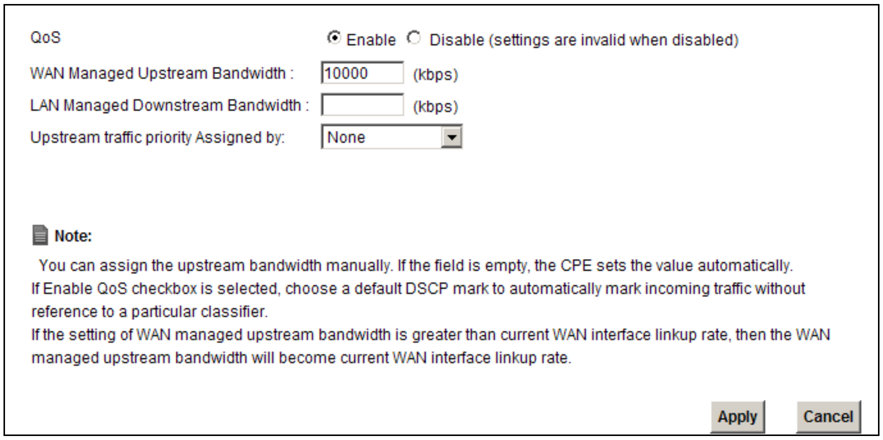
- Configure a queue to assign the highest priority queue (1) to e-mail traffic going to the WAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the Device.



1 Click **Network Setting > QoS > General** and select **Enable**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Device automatically determine this figure). Click **Apply**.



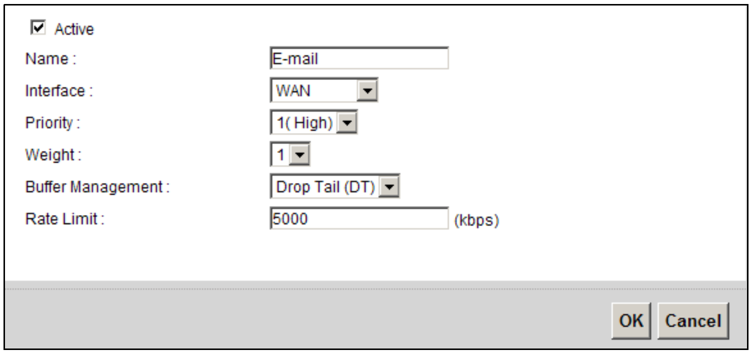
QoS	● Enable ○ Disable (settings are invalid when disabled)
WAN Managed Upstream Bandwidth :	10000 (kbps)
LAN Managed Downstream Bandwidth :	(kbps)
Upstream traffic priority Assigned by:	None

Note:

You can assign the upstream bandwidth manually. If the field is empty, the CPE sets the value automatically.
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

2 Click **Queue Setup** > **Add new Queue** to create a new queue. In the screen that opens, check **Active** and enter or select the following values:

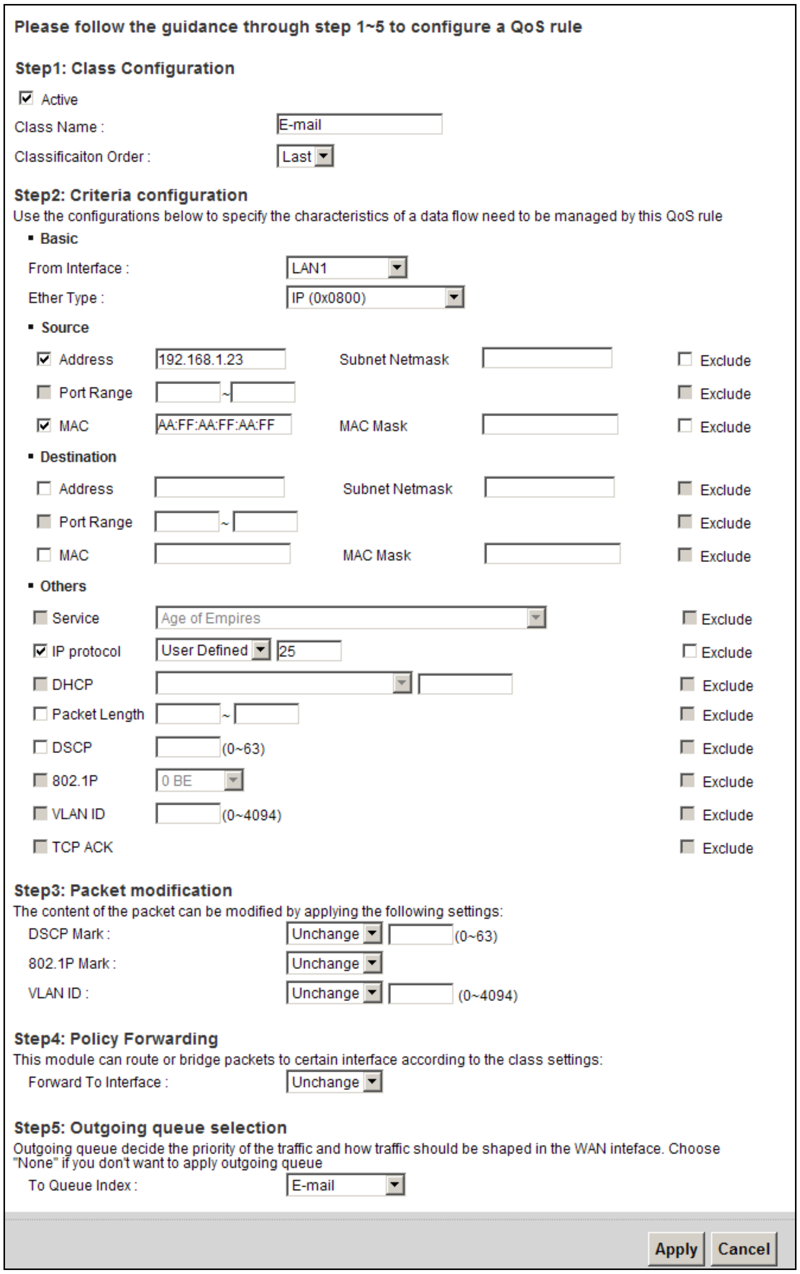
- **Name**: E-mail
- **Interface**: WAN
- **Priority**: 1 (High)
- **Weight**: 8
- **Rate Limit**: 5,000 (kbps)



☑ Active

Name :	E-mail
Interface :	WAN
Priority :	1(High)
Weight :	1
Buffer Management :	Drop Tail (DT)
Rate Limit :	5000 (kbps)

3 Click **Class Setup** > **Add new Classifier** to create a new class. Check **Active** and follow the settings as shown in the screen below.



Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

☑ Active

Class Name : E-mail

Classificaiton Order : Last

Step2: Criteria configuration

Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- **Basic**

From Interface : LAN1

Ether Type : IP (0x0800)

- **Source**

☑ Address	192.168.1.23	Subnet Netmask		□ Exclude
□ Port Range	~			□ Exclude
☑ MAC	AA:FF:AA:FF:AA:FF	MAC Mask		□ Exclude

- **Destination**

□ Address		Subnet Netmask		□ Exclude
□ Port Range	~			□ Exclude
□ MAC		MAC Mask		□ Exclude

- **Others**

□ Service	Age of Empires	□ Exclude
☑ IP protocol	User Defined 25	□ Exclude
□ DHCP		□ Exclude
□ Packet Length	~	□ Exclude
□ DSCP	(0~63)	□ Exclude
□ 802.1P	0 BE	□ Exclude
□ VLAN ID	(0~4094)	□ Exclude
□ TCP ACK		□ Exclude

Step3: Packet modification

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

DSCP Mark : Unchange (0~63)

802.1P Mark : Unchange

VLAN ID : Unchange (0~4094)

Step4: Policy Forwarding

This module can route or bridge packets to certain interface according to the class settings:

Forward To Interface : Unchange

Step5: Outgoing queue selection

Outgoing queue decide the priority of the traffic and how traffic should be shaped in the WAN inteface. Choose "None" if you don't want to apply outgoing queue

To Queue Index : E-mail

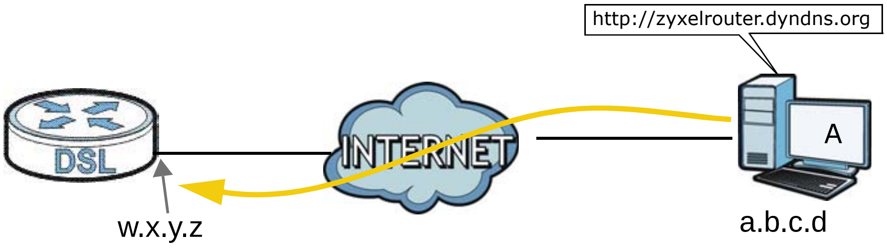
Class Name	Give a class name to this traffic, such as **E-mail** in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **LAN1** for this example.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.
MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
To Queue Index	Link this to an item in the **Network Setting > QoS > Queue Setup** screen, which is the **E-mail** queue created in this example.

This maps e-mail traffic coming from port 25 to the highest priority, which you have created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to the **E-mail** queue (see the **Source** fields).

4 Verify that the queue setup works by checking **Network Setting > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.

4.9 Access the Device Using DDNS

If you connect your Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

4.9.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

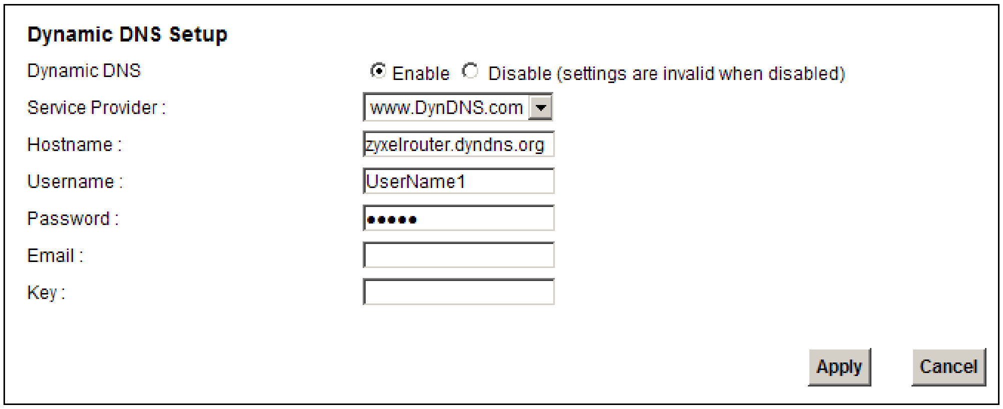
- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your Device is currently using. You can find the IP address on the Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the Device later.

4.9.2 Configuring DDNS on Your Device

Configure the following settings in the **Network Setting > DNS > Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).



Dynamic DNS Setup

Dynamic DNS	● Enable ○ Disable (settings are invalid when disabled)
Service Provider :	www.DynDNS.com
Hostname :	zyxelrouter.dyndns.org
Username :	UserName1
Password :	●●●●●
Email :	
Key :	

Click **Apply**.

4.9.3 Testing the DDNS Setting

Now you should be able to access the Device from the Internet. To test this:

1. Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

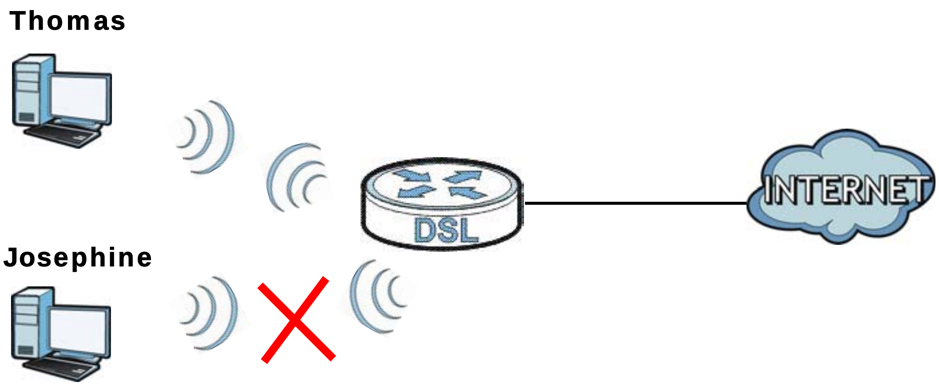
2. Type **http://zyxelrouter.dyndns.org** and press [Enter].

3. The Device’s login page should appear. You can then log into the Device and manage it.

4.10 Configuring the MAC Address Filter

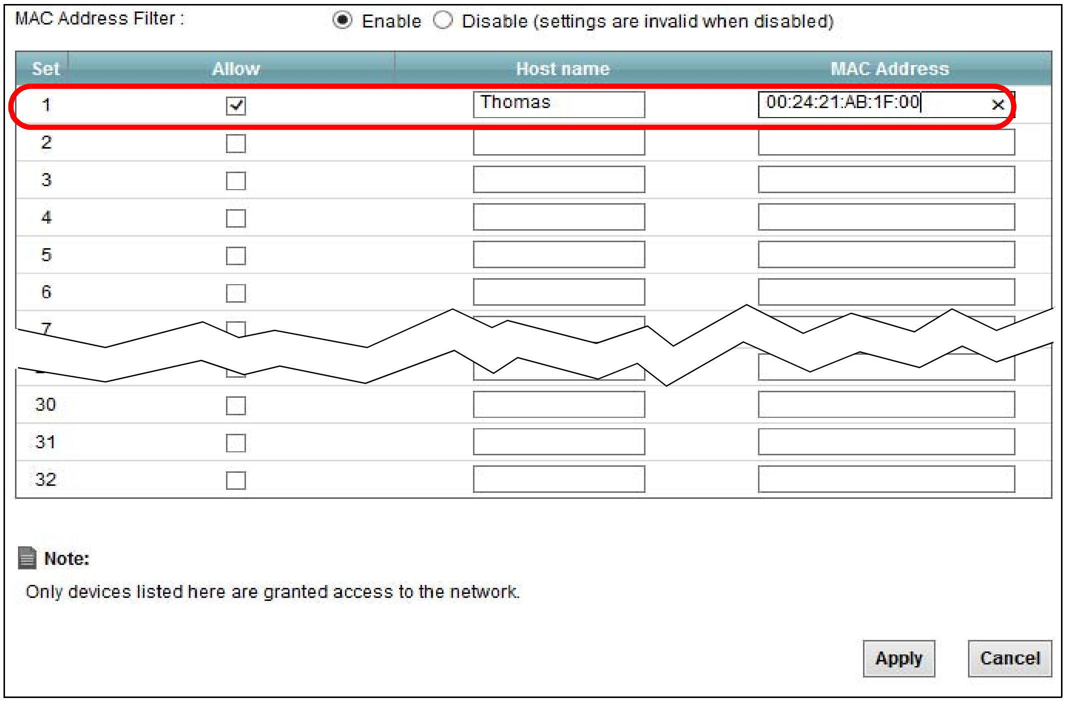
Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



1 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.

2 Select **Allow**. Then enter the host name and MAC address of Thomas' computer in this screen. Click **Apply**.



MAC Address Filter : ● Enable ○ Disable (settings are invalid when disabled)

Set	Allow	Host name	MAC Address
1	☑	Thomas	00:24:21:AB:1F:00
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
30	□		
31	□		
32	□		

Note:

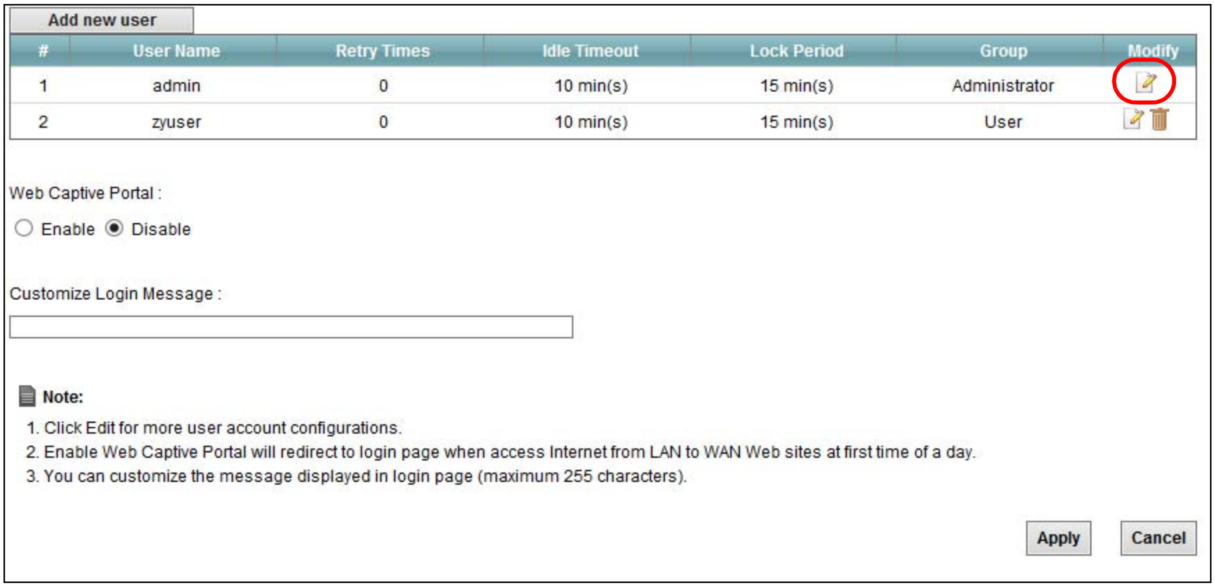
Only devices listed here are granted access to the network.

Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the Device.

4.11 Access Your Shared Files From a Computer

Here is how to enable the Samba feature on the Device and access a file storage device connected to the Device’s USB port.

1 Log into the web configurator and go to the **Maintenance** > **User Account** screen. Click the **Edit** icon on the account you are currently using. In this example, the account in use is **admin**. Click the Edit icon next to it.



#	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	admin	0	10 min(s)	15 min(s)	Administrator	
2	zyuser	0	10 min(s)	15 min(s)	User	

Web Captive Portal :

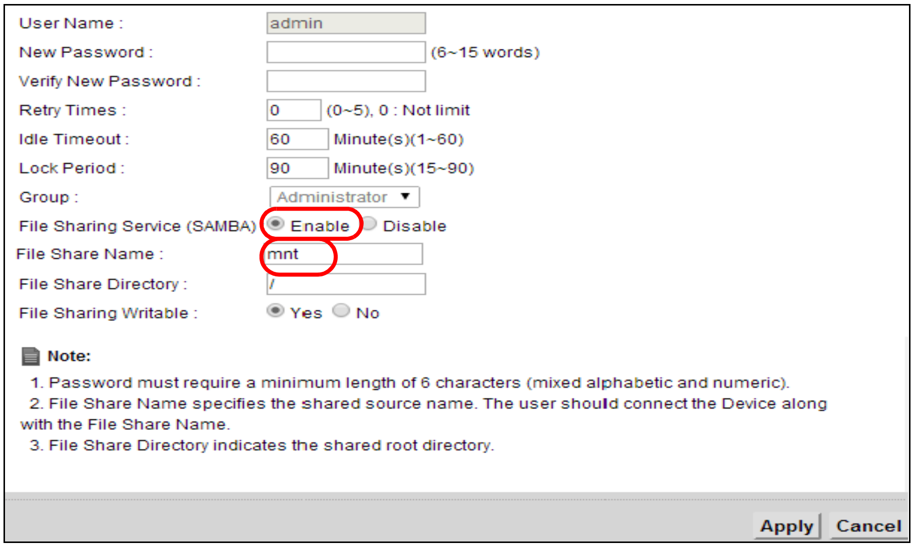
○ Enable ● Disable

Customize Login Message :

Note:

1. Click Edit for more user account configurations.
2. Enable Web Captive Portal will redirect to login page when access Internet from LAN to WAN Web sites at first time of a day.
3. You can customize the message displayed in login page (maximum 255 characters).

2 Set the **File Sharing Service (SAMBA)** feature to **Enable** to allow uses to access shared files in USB storage. Enter **mnt** as the **File Share Name**. Click **Apply**.

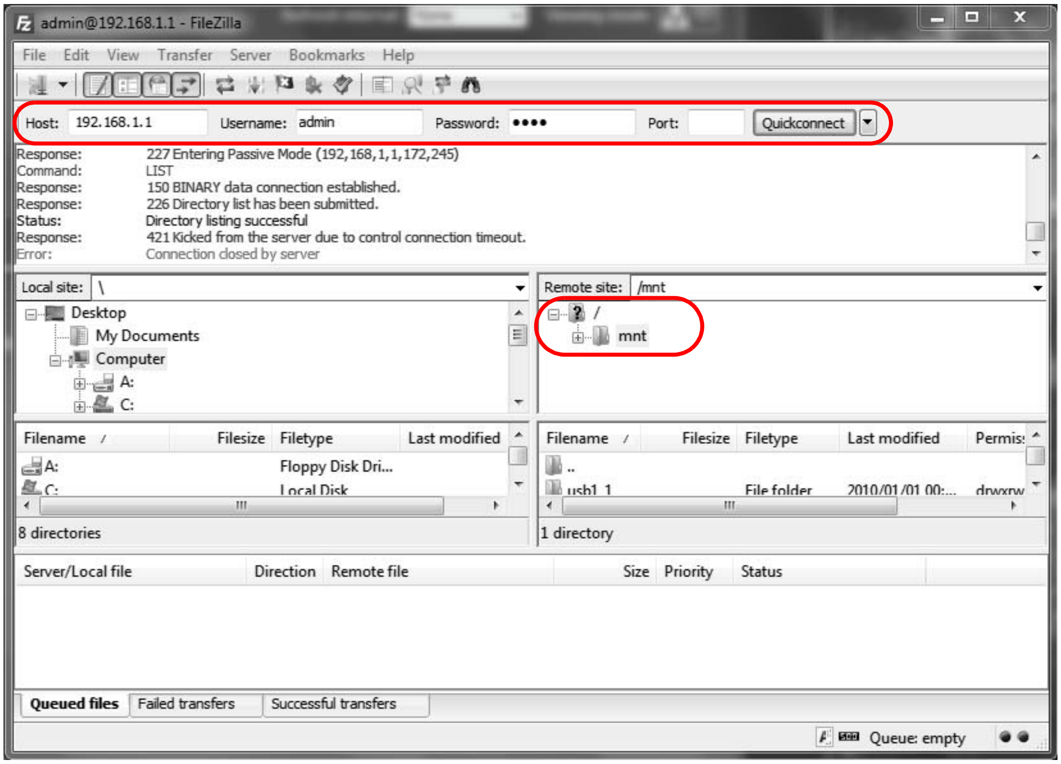


User Name :	admin
New Password :	(6~15 words)
Verify New Password :	
Retry Times :	0 (0~5), 0 : Not limit
Idle Timeout :	60 Minute(s)(1~60)
Lock Period :	90 Minute(s)(15~90)
Group :	Administrator
File Sharing Service (SAMBA) :	● Enable ○ Disable
File Share Name :	mnt
File Share Directory :	/
File Sharing Writable :	● Yes ○ No

Note:

1. Password must require a minimum length of 6 characters (mixed alphabetic and numeric).
2. File Share Name specifies the shared source name. The user should connect the Device along with the File Share Name.
3. File Share Directory indicates the shared root directory.

3 In this example, the FileZilla program is used to browse shared files. In FileZilla, enter the IP address of the Device (the default is 192.168.1.1), your account’s user name and password and port 21 and click **Quickconnect**. A screen asking for password authentication appears.



Host: 192.168.1.1 Username: admin Password: •••• Port:

```
Response:   227 Entering Passive Mode (192,168,1,1,172,245)
Command:    LIST
Response:   150 BINARY data connection established.
Response:   226 Directory list has been submitted.
Status:     Directory listing successful
Response:   421 Kicked from the server due to control connection timeout.
Error:      Connection closed by server
```

Filename /	Filesize	Filetype	Last modified
A:		Floppy Disk Dri...	
C:		Local Disk	

8 directories

Filename /	Filesize	Filetype	Last modified	Permis:
..				
usb1_1		File folder	2010/01/01 00:...	drwxrw

1 directory

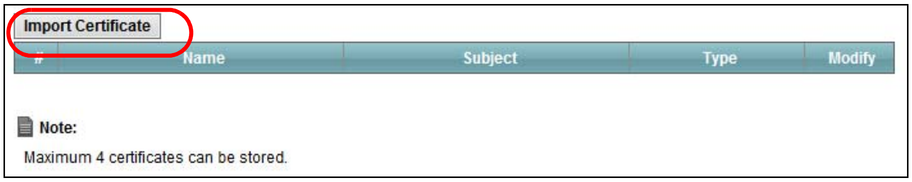
Server/Local file	Direction	Remote file	Size	Priority	Status

4 Once you log in the USB device displays in the **mnt** folder.

4.12 Certificate Configuration for VPN

You may generate a self-signed Certification Authority (CA) certificate using a third party tool or get an official CA certificate from any trusted certificate agent. In this tutorial, a self-signed CA certificate (cacert.pem) was created by using the openssl command in Fedora 10.

1 First, you need to import the CA certificate. Go to the **Security** > **Certificates** > **Trusted CA** screen and click **Import Certificate**.

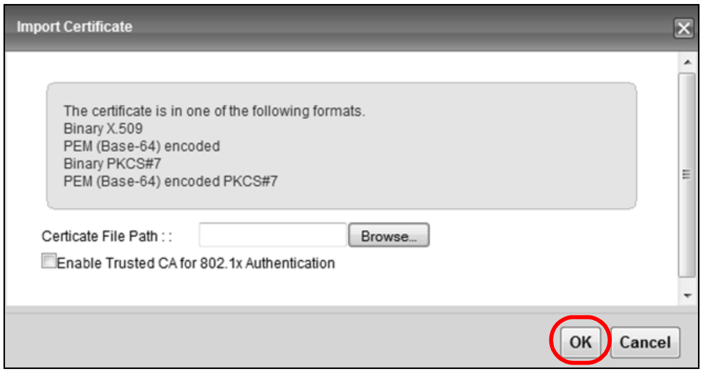


#	Name	Subject	Type	Modify

Note:

Maximum 4 certificates can be stored.

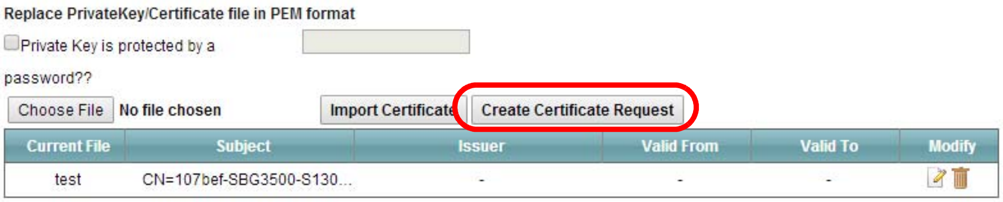
2 Browse the directory in Fedora, or another system, which contains your CA certificate (e.g., cacert.pem), then click **OK**.


Import Certificate

The certificate is in one of the following formats.
Binary X.509
PEM (Base-64) encoded
Binary PKCS#7
PEM (Base-64) encoded PKCS#7

Certicate File Path : :
□Enable Trusted CA for 802.1x Authentication

3 In the **Security** > **Certificates** > **Local Certificates** screen, click **Create Certificate Request**.

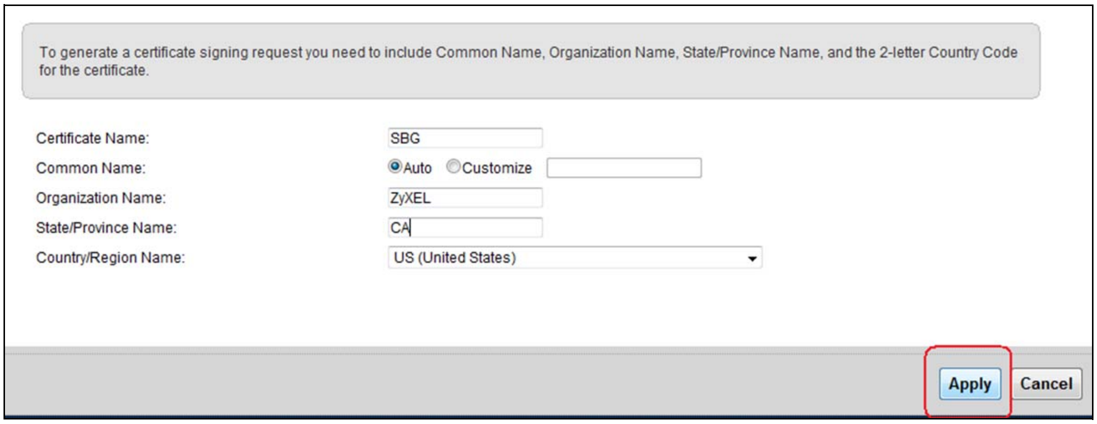

Replace PrivateKey/Certificate file in PEM format

□Private Key is protected by a password??

No file chosen

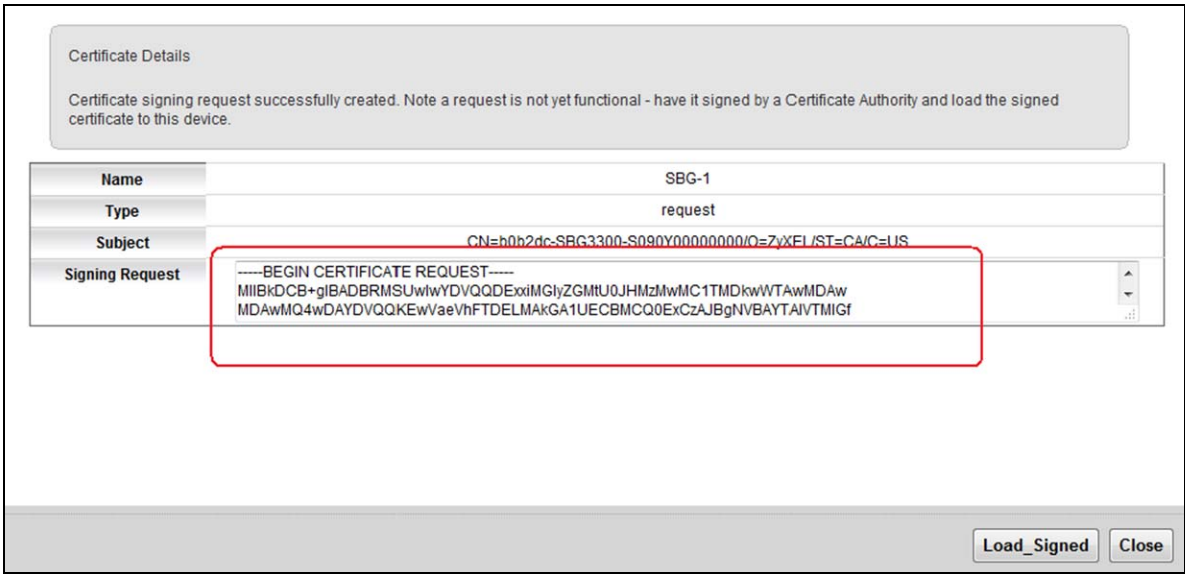
Current File	Subject	Issuer	Valid From	Valid To	Modify
test	CN=107bef-SBG3500-S130...	-	-	-	

4 Enter your information as shown in the following screen and click **Apply**.


To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:	SBG
Common Name:	● Auto ○ Customize
Organization Name:	ZyXEL
State/Province Name:	CA
Country/Region Name:	US (United States)

5 The contents of the certificate display in the **View Certificate** screen. Copy the **Signing Request** section and paste it to a file (for example, sbg.req) in Fedora, or another system, which contains your original CA certificate.



Certificate Details

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	SBG-1
Type	request
Subject	CN=b0b2dc-SBG3300-S090Y00000000/O=ZyXEL/ST=CA/C=US
Signing Request	-----BEGIN CERTIFICATE REQUEST----- MIIBkDCB+gIBADBRMSUwIwYDVQQDExxiMGIyZGMtU0JHMzMwMC1TMDkwWTAwMDAw MDAwMQ4wDAYDVQQKEwVaeVhFTDELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMIGf

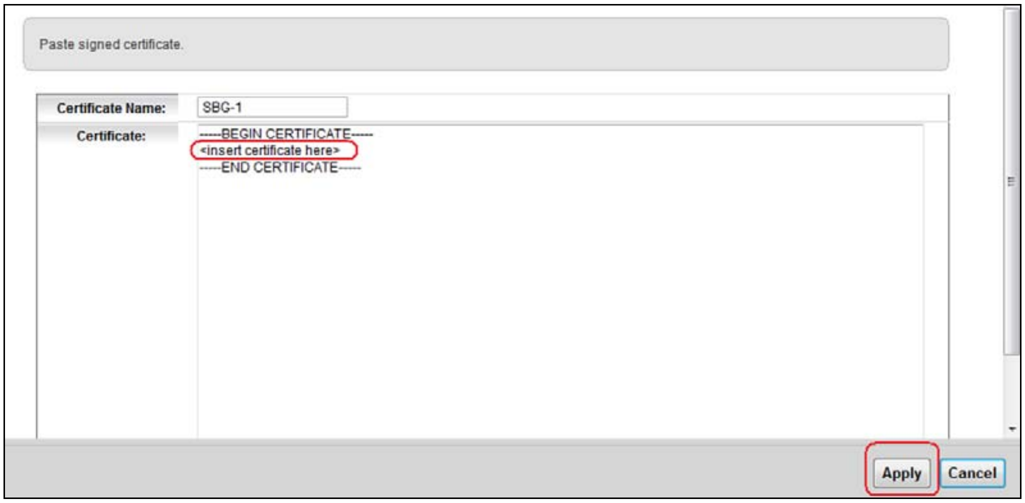
6 In Fedora, issue the following openssl command to generate the host certificate for the Device:

```
openssl ca -config ./openssl.conf -policy policy_anything -out sbg.pem
-infiles sbg.req
```

7 Click the **Load_Signed** button in the **View Certificate** screen.

8 Cut the contents of sbg.pem (only the binary portion between BEGIN CERTIFICATE and END CERTIFICATE). You can use "vi" or your favorite text editor to cut the portion, but do not use the "cat" command.

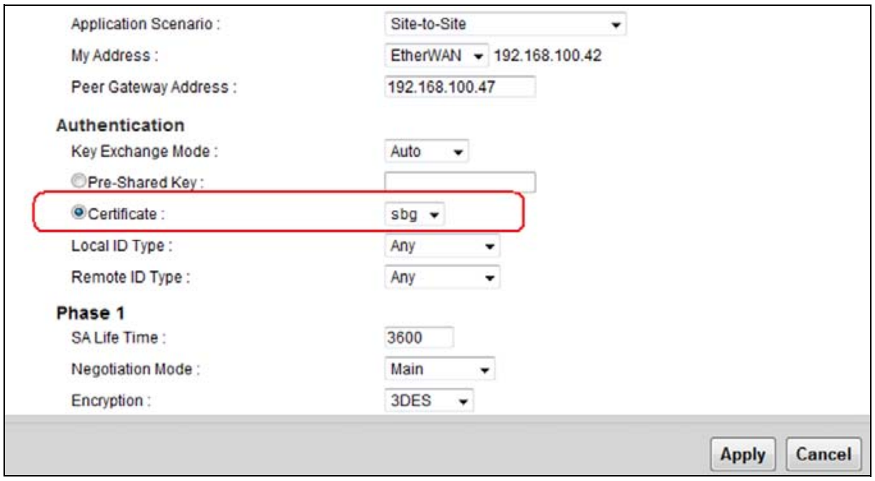
9 Paste it to the indicated part of the **Certificate** section in the **View Certificate** screen. Click **Apply**.



Paste signed certificate.

Certificate Name:	SBG-1
Certificate:	-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----

10 Now you may configure VPN to use the new certificate for authentication in the **VPN** > **IPSec VPN** > **Monitor** screen.



Application Scenario : Site-to-Site
My Address : EtherWAN 192.168.100.42
Peer Gateway Address : 192.168.100.47

Authentication
Key Exchange Mode : Auto
○ Pre-Shared Key :
● Certificate : sbg
Local ID Type : Any
Remote ID Type : Any

Phase 1
SA Life Time : 3600
Negotiation Mode : Main
Encryption : 3DES

4.13 Examples of Configuring IPSec VPN Rules

The first two examples show how to configure Site-to-Site rules with pre-shared secrets. The first example uses 3DES encryption and the second one uses AES128.

The third example shows how to configure a Site-to-Site with Dynamic Peer rule using pre-shared secret keys.

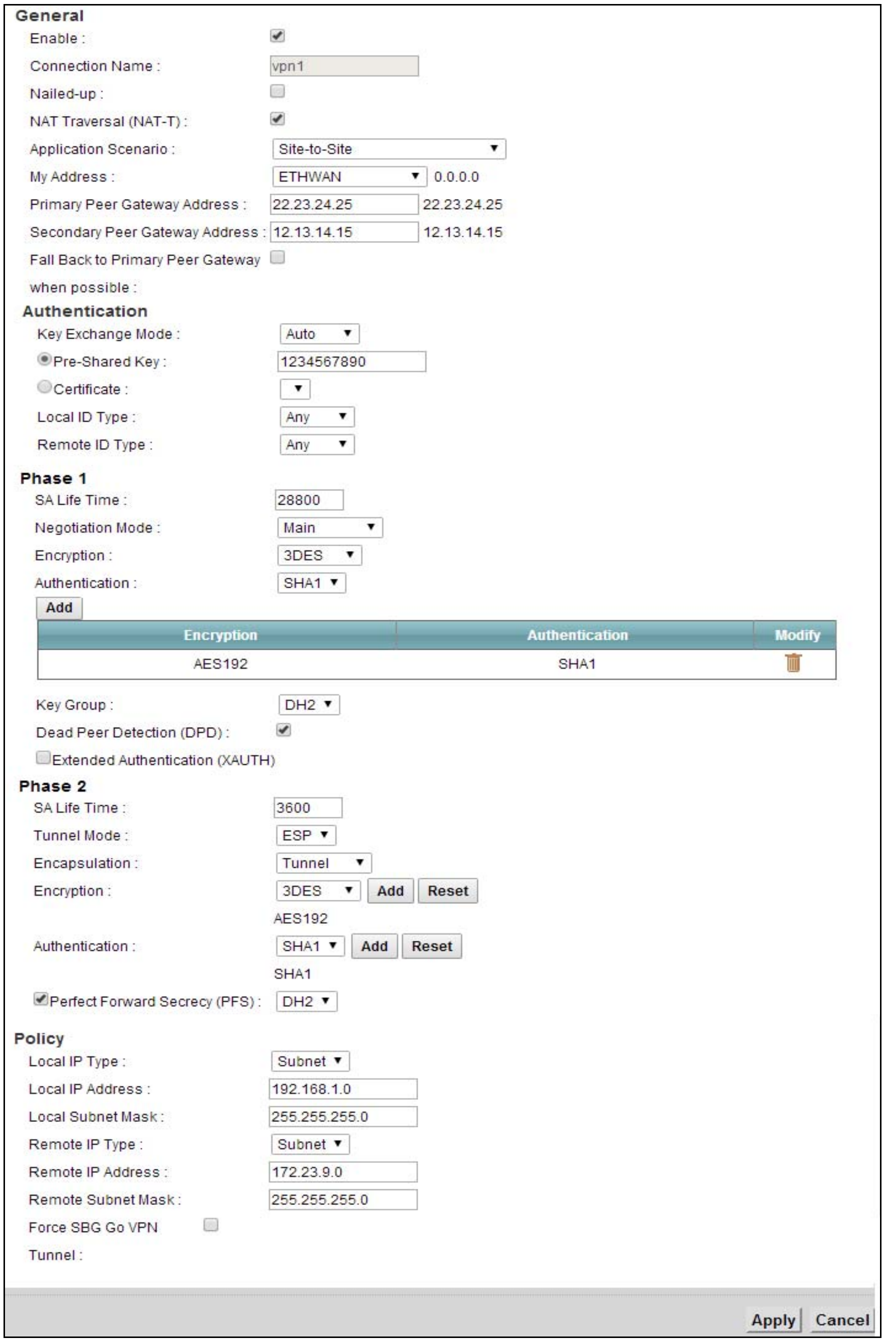
Finally, the fourth example shows how to configure remote access using pre-shared secrets.

4.13.1 Example 1: Use 3DES Encryption

1 Click the **Add New Entry** button in the **VPN** > **IPSec VPN** > **Setup** screen and enter the following parameters:

General	
Connection Name	vpn1
Application Scenario	Site-to-Site
My Address	ETHWAN
Peer Gateway Address	22.23.24.25
Authentication	
Key Exchange Mode	Auto
Pre-Shared Key	1234567890
Phase 1	
SA Life Time	28800
Negotiation Mode	Main
Encryption	3DES

Authentication	SHA1
Key Group	DH2
Phase 2	
SA Life Time	3600
Tunnel Mode	ESP
Encapsulation	Tunnel
Encryption	3DES
Authentication	SHA1
PFS	DH2
Policy	
Local IP Type	Subnet
Local IP Address	192.168.1.0
Local Subnet Mask	255.255.255.0
Remote IP Type	Subnet
Remote IP Address	172.23.9.0
Remote Subnet Mask	255.255.255.0



General

Enable : ☑

Connection Name : vpn1

Nailed-up : □

NAT Traversal (NAT-T) : ☑

Application Scenario : Site-to-Site ▼

My Address : ETHWAN ▼ 0.0.0.0

Primary Peer Gateway Address : 22.23.24.25 22.23.24.25

Secondary Peer Gateway Address : 12.13.14.15 12.13.14.15

Fall Back to Primary Peer Gateway when possible : □

Authentication

Key Exchange Mode : Auto ▼

● Pre-Shared Key : 1234567890

○ Certificate : ▼

Local ID Type : Any ▼

Remote ID Type : Any ▼

Phase 1

SA Life Time : 28800

Negotiation Mode : Main ▼

Encryption : 3DES ▼

Authentication : SHA1 ▼

Encryption	Authentication	Modify
AES192	SHA1	🗑

Key Group : DH2 ▼

Dead Peer Detection (DPD) : ☑

□ Extended Authentication (XAUTH)

Phase 2

SA Life Time : 3600

Tunnel Mode : ESP ▼

Encapsulation : Tunnel ▼

Encryption : 3DES ▼ Add Reset
AES192

Authentication : SHA1 ▼ Add Reset
SHA1

☑ Perfect Forward Secrecy (PFS) : DH2 ▼

Policy

Local IP Type : Subnet ▼

Local IP Address : 192.168.1.0

Local Subnet Mask : 255.255.255.0

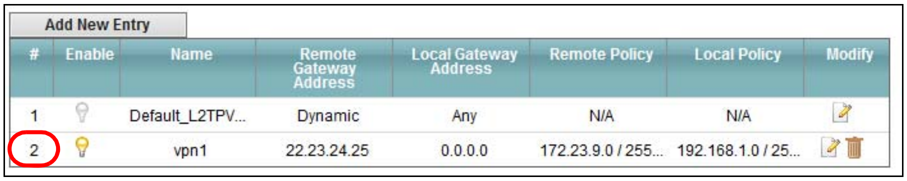
Remote IP Type : Subnet ▼

Remote IP Address : 172.23.9.0

Remote Subnet Mask : 255.255.255.0

Force SBG Go VPN Tunnel : □

You can see the new IPSec VPN rule you've just created in the **VPN** > **IPSec VPN** > **Monitor** screen.



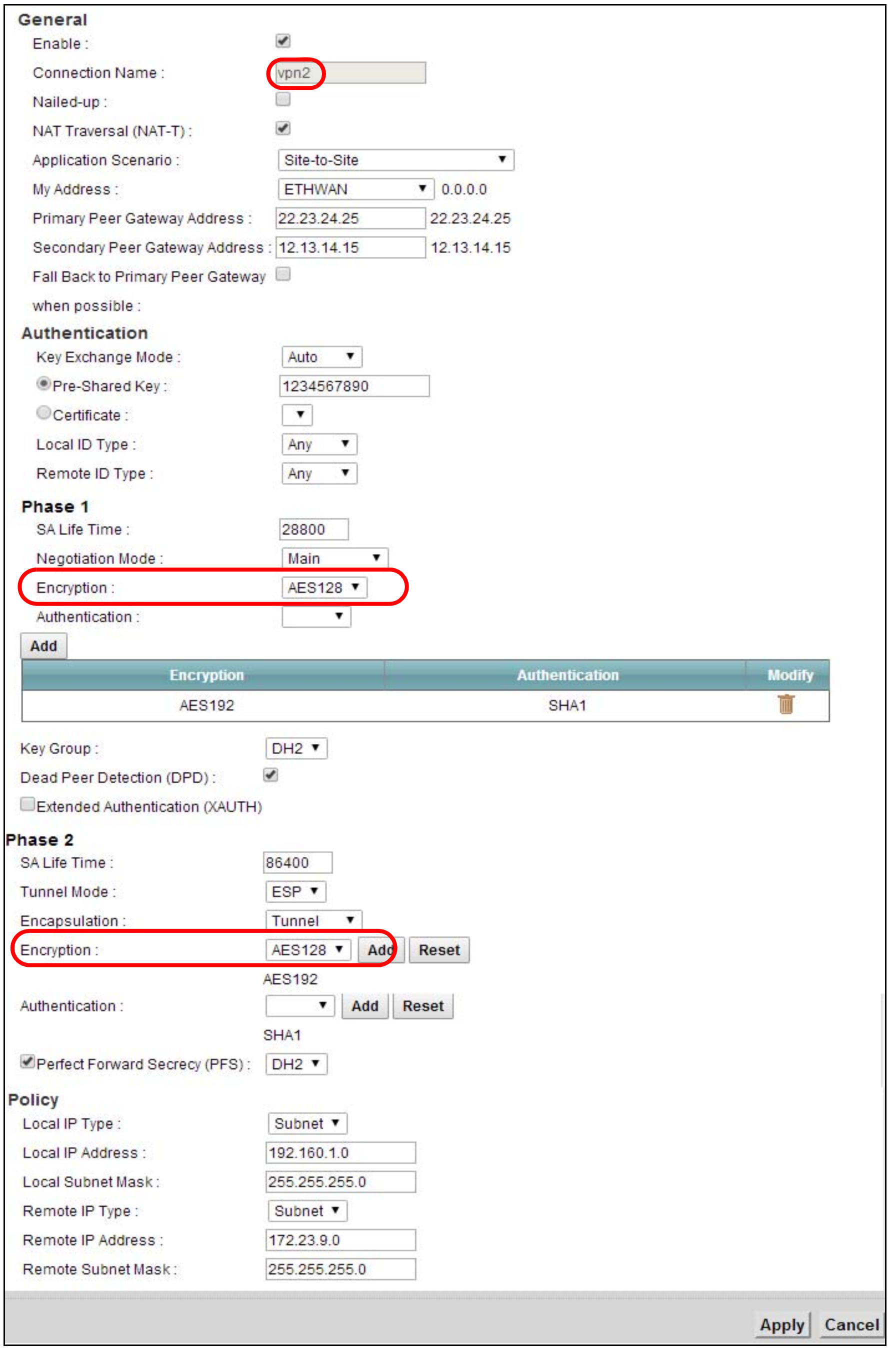
#	Enable	Name	Remote Gateway Address	Local Gateway Address	Remote Policy	Local Policy	Modify
1	○	Default_L2TPV...	Dynamic	Any	N/A	N/A	✎
2	●	vpn1	22.23.24.25	0.0.0.0	172.23.9.0 / 255...	192.168.1.0 / 25...	✎ 🗑

4.13.2 Example 2: Use AES128 Encryption

Here is another example of creating a Gateway-to-Gateway IPSec VPN rule with pre-shared secrets.

1 Click the **Add New Entry** button in the **VPN** > **IPSec VPN** > **Setup** screen.

2 Enter **vpn2** as the **Connection Name**. Remove the existing encryption by clicking **Remove** icon or **Reset** button. Then select **AES128** and click the **Add** button in the **Encryption** fields of phase 1 and 2. Other parameters are the same as example 1's.



General

Enable : ☑

Connection Name : vpn2

Nailed-up : □

NAT Traversal (NAT-T) : ☑

Application Scenario : Site-to-Site

My Address : ETHWAN 0.0.0.0

Primary Peer Gateway Address : 22.23.24.25 22.23.24.25

Secondary Peer Gateway Address : 12.13.14.15 12.13.14.15

Fall Back to Primary Peer Gateway when possible : □

Authentication

Key Exchange Mode : Auto

● Pre-Shared Key : 1234567890

○ Certificate :

Local ID Type : Any

Remote ID Type : Any

Phase 1

SA Life Time : 28800

Negotiation Mode : Main

Encryption : AES128

Authentication :

Add

Encryption	Authentication	Modify
AES192	SHA1	🗑

Key Group : DH2

Dead Peer Detection (DPD) : ☑

□ Extended Authentication (XAUTH)

Phase 2

SA Life Time : 86400

Tunnel Mode : ESP

Encapsulation : Tunnel

Encryption : AES128 Add Reset

AES192

Authentication : Add Reset

SHA1

☑ Perfect Forward Secrecy (PFS) : DH2

Policy

Local IP Type : Subnet

Local IP Address : 192.160.1.0

Local Subnet Mask : 255.255.255.0

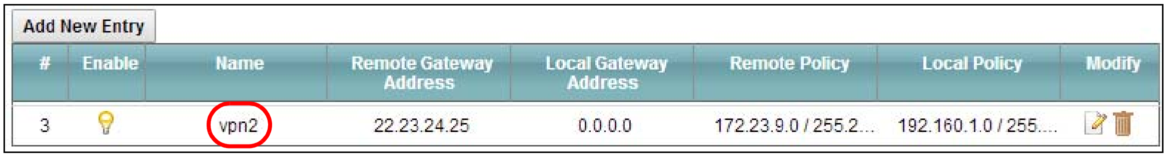
Remote IP Type : Subnet

Remote IP Address : 172.23.9.0

Remote Subnet Mask : 255.255.255.0

Apply Cancel

3 You can see the new IPSec VPN rule you've just created in the **VPN** > **IPSec VPN** > **Monitor** screen.

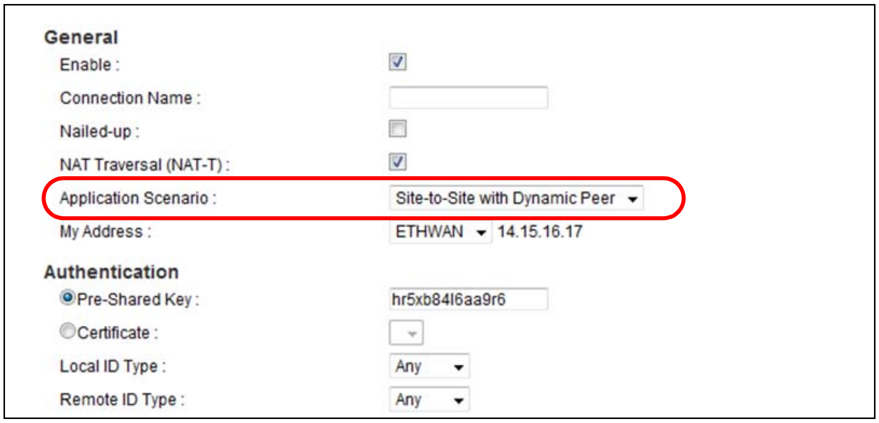


Add New Entry

#	Enable	Name	Remote Gateway Address	Local Gateway Address	Remote Policy	Local Policy	Modify
3	💡	vpn2	22.23.24.25	0.0.0.0	172.23.9.0 / 255.2...	192.160.1.0 / 255....	✎ 🗑

4.13.3 Example 3: Configuring a Site-to-Site with Dynamic Peer Rule

Select **Site-to-Site with Dynamic Peer** in the **Application Scenario** field in the **General** section. Other parameters are the same as example 1's.



General

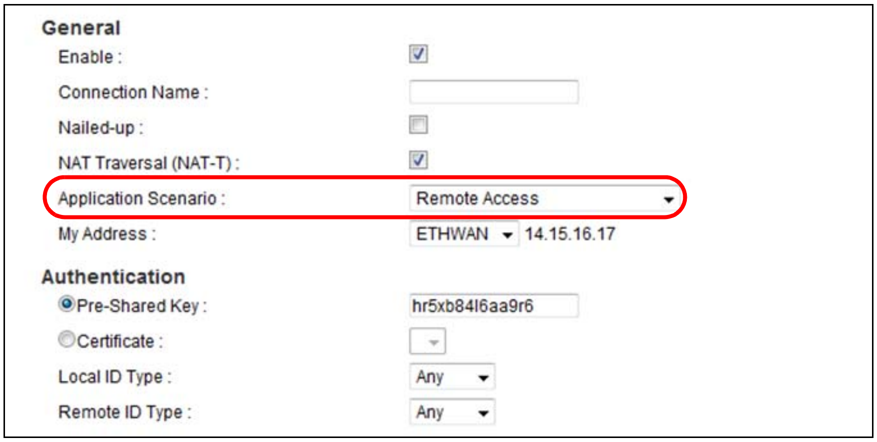
Enable :	☑
Connection Name :	
Nailed-up :	□
NAT Traversal (NAT-T) :	☑
Application Scenario :	Site-to-Site with Dynamic Peer
My Address :	ETHWAN 14.15.16.17

Authentication

● Pre-Shared Key :	hr5xb84l6aa9r6
○ Certificate :	
Local ID Type :	Any
Remote ID Type :	Any

4.13.4 Example 4: Configuring a Remote Access Rule

Select **Remote Access** in the **Application Scenario** field in the **General** section. Other parameters are the same as example 1's.



General

Enable :	☑
Connection Name :	
Nailed-up :	□
NAT Traversal (NAT-T) :	☑
Application Scenario :	Remote Access
My Address :	ETHWAN 14.15.16.17

Authentication

● Pre-Shared Key :	hr5xb84l6aa9r6
○ Certificate :	
Local ID Type :	Any
Remote ID Type :	Any

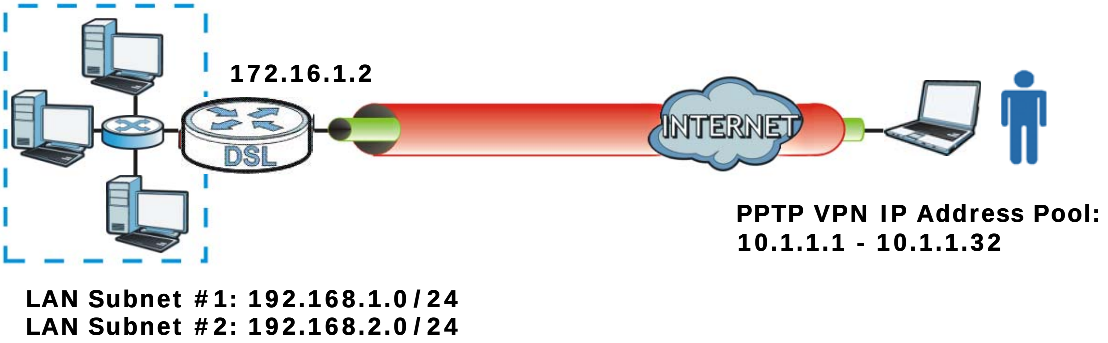
Note: The **Peer Gateway Address** is not shown in the screen because it is an unknown IP address to the remote access VPN client.

Note: The policy for the remote VPN client is not shown in the screen because it is an unknown to the remote access VPN client.

4.14 PPTP VPN Tutorial

The example uses the following settings in setting up a basic PPTP VPN tunnel.

Figure 15 PPTP VPN Example


172.16.1.2
DSL
INTERNET
PPTP VPN IP Address Pool:
10.1.1.1 - 10.1.1.32
LAN Subnet #1: 192.168.1.0/24
LAN Subnet #2: 192.168.2.0/24

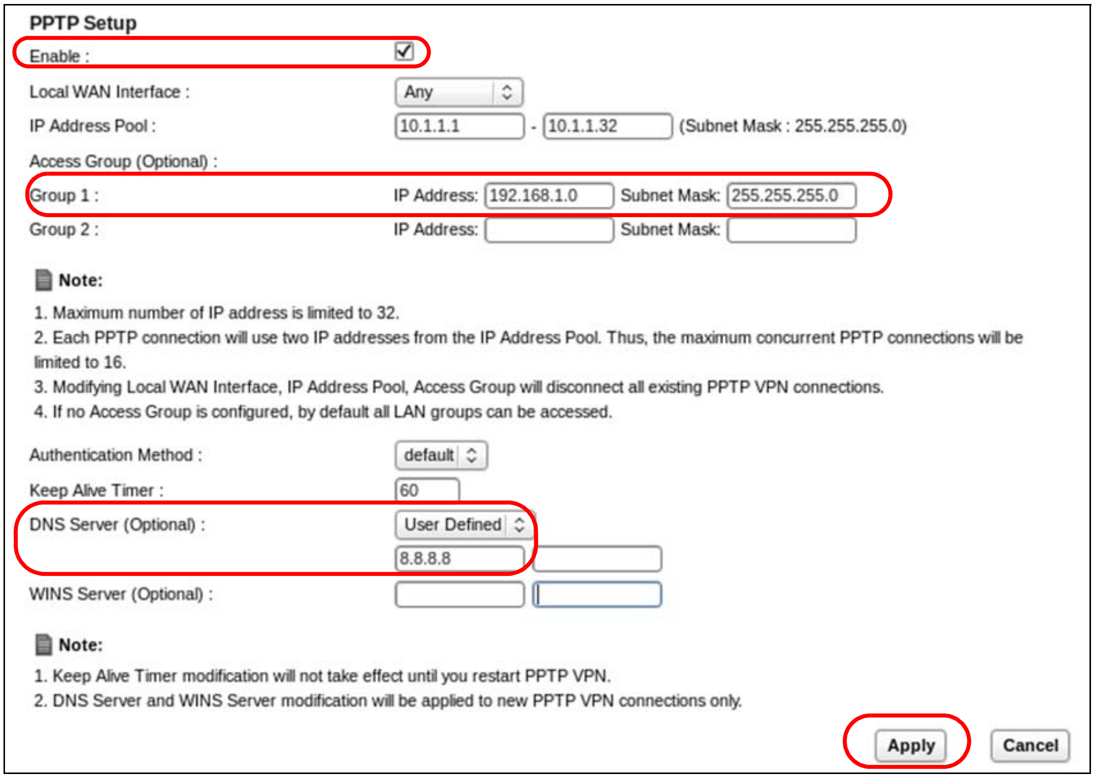
- The Device has a static IP address of **172.16.1.2** for the DSL WAN interface.
- The remote user has a dynamic IP address and connects through the Internet.
- Use the default IP address pool to assign the remote users a point-to-point IP addresses from **10.1.1.1** to **10.1.1.32** for use in the PPTP VPN tunnel.
- The access group configuration allows the remote user to access only the **LAN subnet #1 192.168.1.0/24**.

4.14.1 Configuring PPTP VPN Setup (Server)

1.Go to the **VPN** > **PPTP VPN** > **Setup** screen and configure the following.

- Select the **Enable** checkbox.
- Set **Access Group 1** to **192.168.1.0/255.255.255.0**.
- Select **DNS** as **User Defined** and enter a DNS server address. The DNS server address in this example is **8.8.8.8**.

- Click **Apply**.



PPTP Setup

Enable : ☑

Local WAN Interface : Any

IP Address Pool : 10.1.1.1 - 10.1.1.32 (Subnet Mask : 255.255.255.0)

Access Group (Optional) :

Group 1 : IP Address: 192.168.1.0 Subnet Mask: 255.255.255.0

Group 2 : IP Address: Subnet Mask:

Note:

1. Maximum number of IP address is limited to 32.
2. Each PPTP connection will use two IP addresses from the IP Address Pool. Thus, the maximum concurrent PPTP connections will be limited to 16.
3. Modifying Local WAN Interface, IP Address Pool, Access Group will disconnect all existing PPTP VPN connections.
4. If no Access Group is configured, by default all LAN groups can be accessed.

Authentication Method : default

Keep Alive Timer : 60

DNS Server (Optional) : User Defined

8.8.8.8

WINS Server (Optional) :

Note:

1. Keep Alive Timer modification will not take effect until you restart PPTP VPN.
2. DNS Server and WINS Server modification will be applied to new PPTP VPN connections only.

4.14.2 Configuring PPTP VPN on Windows (Client)

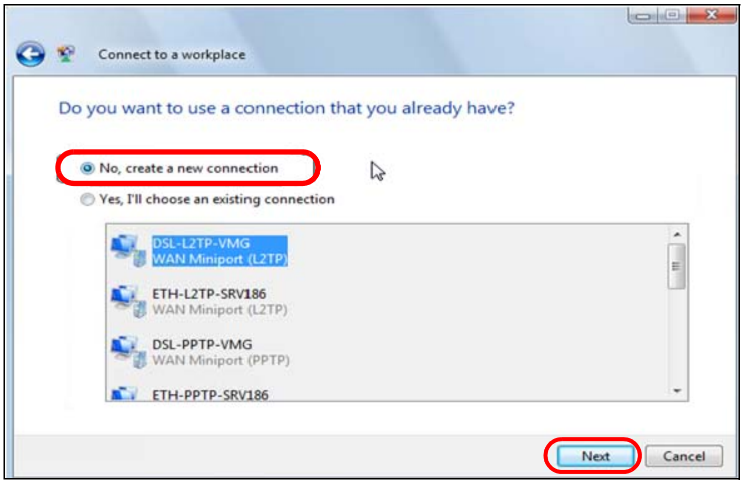
The following sections cover how to configure PPTP in remote user computers using Windows 7, Vista and XP. The example settings in these sections match the PPTP VPN configuration example in Section 4.14 on page 69.

On Windows 7

On Windows 7, do the following to establish a PPTP VPN connection.

1 Click **Start** > **Control Panel** > **Network and Sharing Center** > **Setup a new connection or network** > **Connect to a workplace**. Click **Next**.

2 Select **No, create a new connection**. Click **Next**.



Connect to a workplace

Do you want to use a connection that you already have?

● No, create a new connection

○ Yes, I'll choose an existing connection

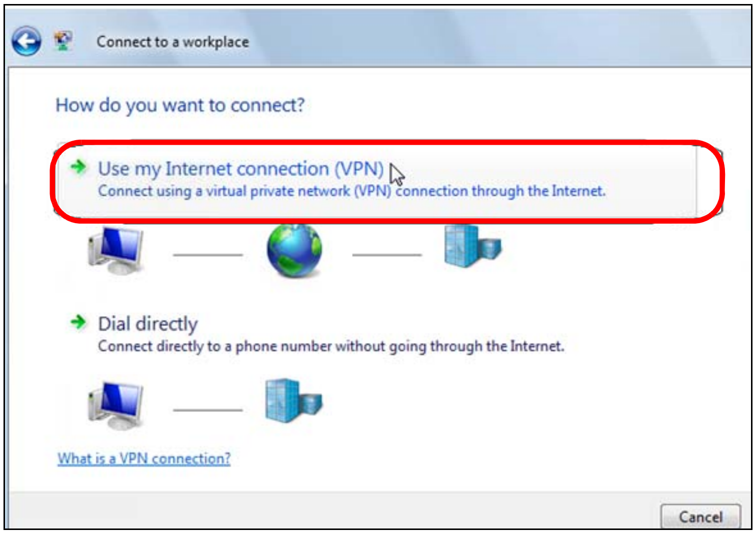
DSL-L2TP-VMG
WAN Miniport (L2TP)

ETH-L2TP-SRV186
WAN Miniport (L2TP)

DSL-PPTP-VMG
WAN Miniport (PPTP)

ETH-PPTP-SRV186

3 Select **Use my Internet connection (VPN)**.



Connect to a workplace

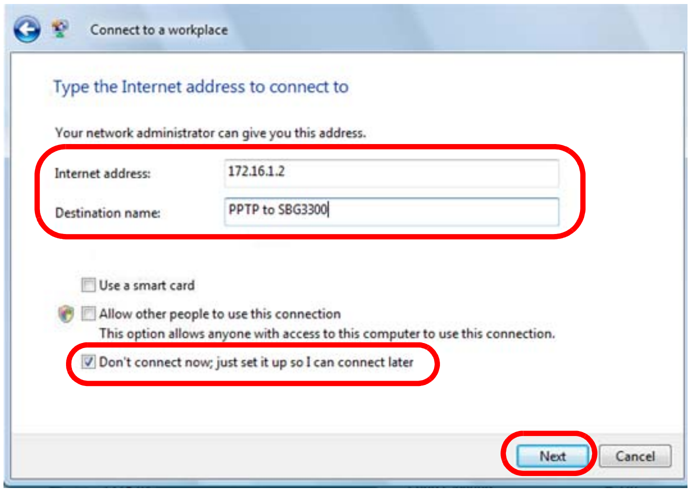
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

4 Enter the domain name or WAN IP Address that you want to connect to **(172.16.1.2** in this example) and give this connection a name. Select **Don't connect now; just set it up so I can connect later**. Click **Next**.



Connect to a workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.2

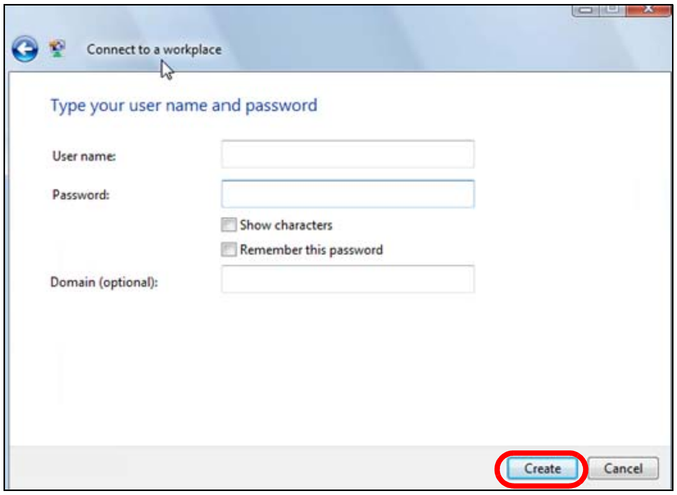
Destination name: PPTP to SBG3300

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

5 Click **Create**. Enter the user name and password later.



Connect to a workplace

Type your user name and password

User name:

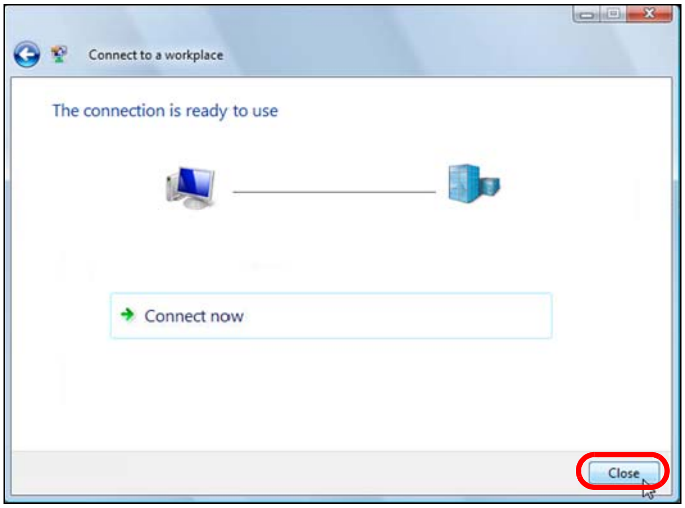
Password:

□ Show characters

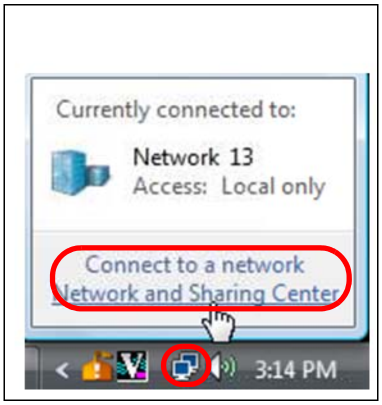
□ Remember this password

Domain (optional):

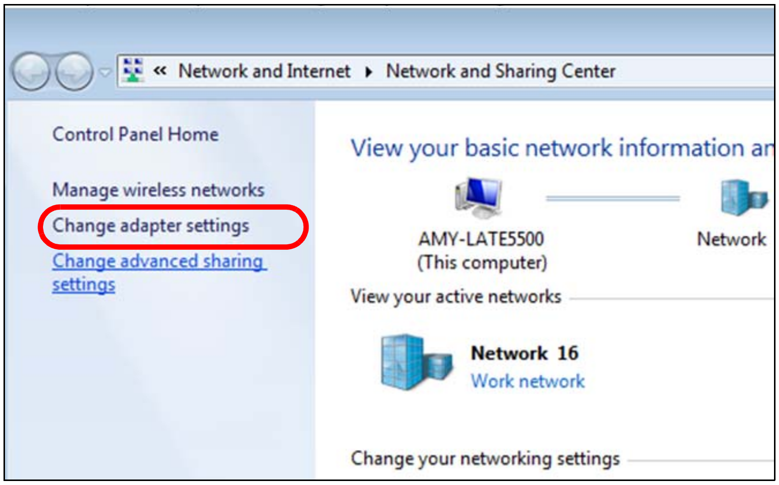
6 Click **Close**. Do not connect yet.



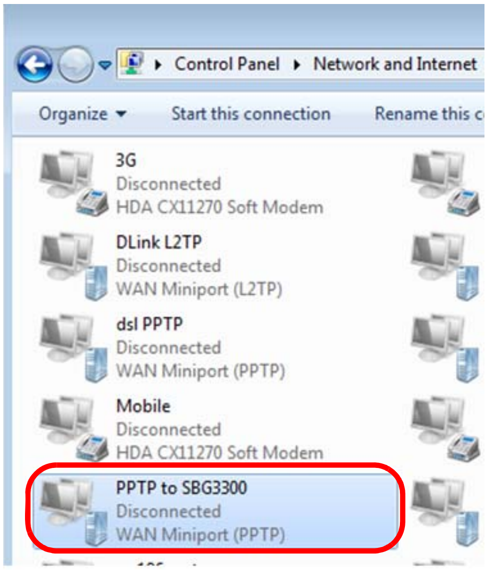
7 Click the **Network** icon in your system tray, then click **Connect to a Network and Sharing Center** on Windows 7.



8 Cick **Change adapter settings**.


« Network and Internet ▸ Network and Sharing Center
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information ar
AMY-LATE5500
(This computer)
Network
View your active networks
Network 16
Work network
Change your networking settings

9 Double-click the new connection icon.



Control Panel ▸ Network and Internet

Organize ▾ Start this connection Rename this c

3G
Disconnected
HDA CX11270 Soft Modem

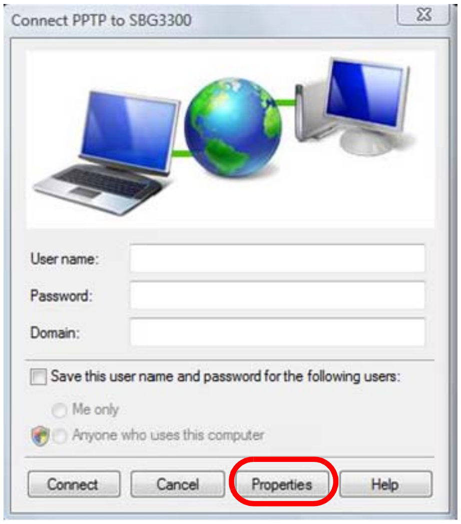
DLink L2TP
Disconnected
WAN Miniport (L2TP)

dsl PPTP
Disconnected
WAN Miniport (PPTP)

Mobile
Disconnected
HDA CX11270 Soft Modem

PPTP to SBG3300
Disconnected
WAN Miniport (PPTP)

10 The connection screen appears. Click **Properties**.



Connect PPTP to SBG3300

User name:

Password:

Domain:

□ Save this user name and password for the following users:

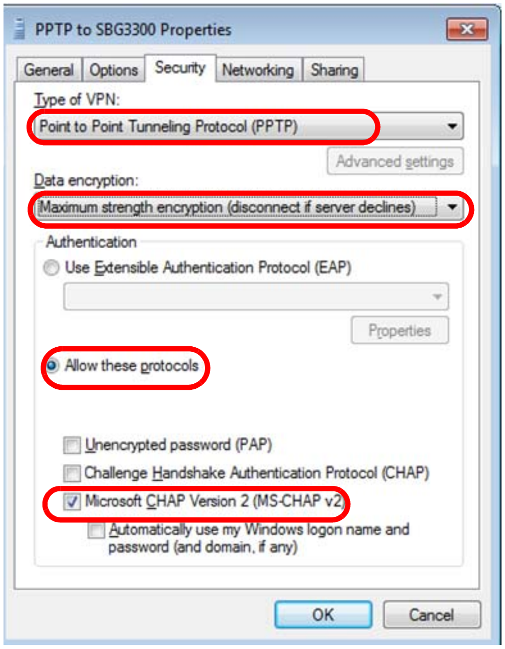
○ Me only

○ Anyone who uses this computer

Connect Cancel Properties Help

11 The **Properties** window appears. Click **Security**.

12 Select **Point to Point Tunneling Protocol (PPTP)** as the **Type of VPN**. Select **Maximum strength encryption (disconnect if server declines)** and the **Allow these protocols** radio button. Select **Microsoft CHAP Version 2 (MS-CHAP v2)** and clear all of the other check boxes. Do not click **OK** yet.



Type of VPN: Point to Point Tunneling Protocol (PPTP)

Data encryption: Maximum strength encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

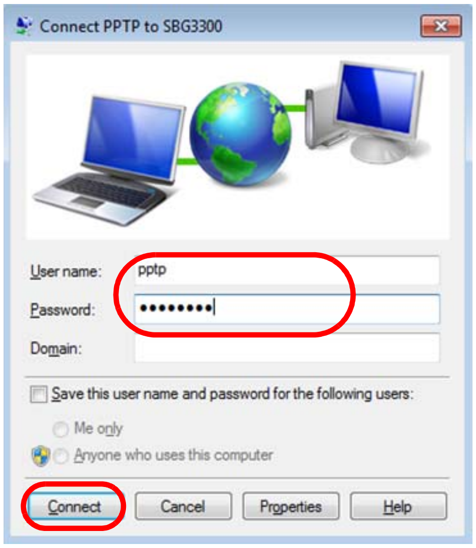
□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

13 In the **Connect** window, enter the username and password of your Device's account. Click **Connect**.



User name: pptp

Password: ••••••••

Domain:

□ Save this user name and password for the following users:

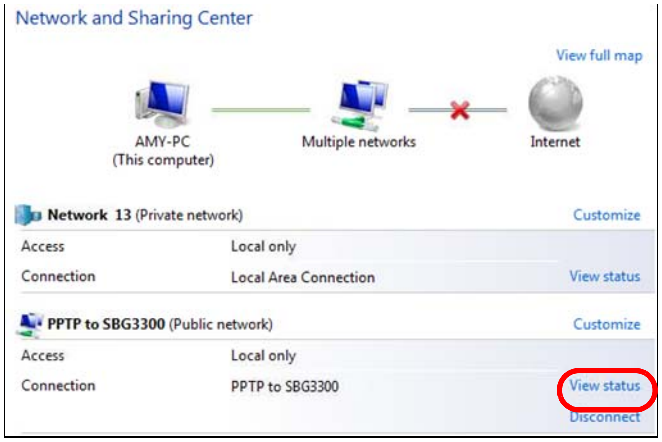
○ Me only

○ Anyone who uses this computer

Note: The user account must have been configured in the **Maintenance** > **User Account** screen. Refer to Chapter 29 on page 300.

14 A window appears while the username and password are verified. The connection is then established.

15 The **Network and Sharing Center** windows appear. You can view the connection status or disconnect the connection. Click **View Status** to open the connection status screen.



Network and Sharing Center

Network 13 (Private network) Customize

Access Local only

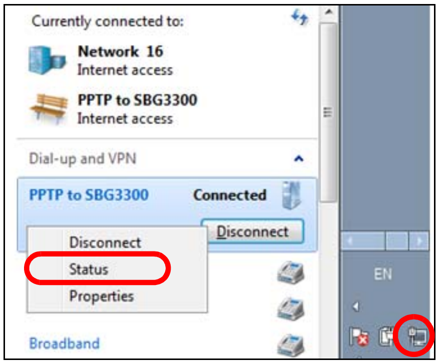
Connection Local Area Connection View status

PPTP to SBG3300 (Public network) Customize

Access Local only

Connection PPTP to SBG3300 View status

16 Click the **Network** icon in your system tray, then right click the PPTP connection and select **Status** to open the connection status screen.



Currently connected to:

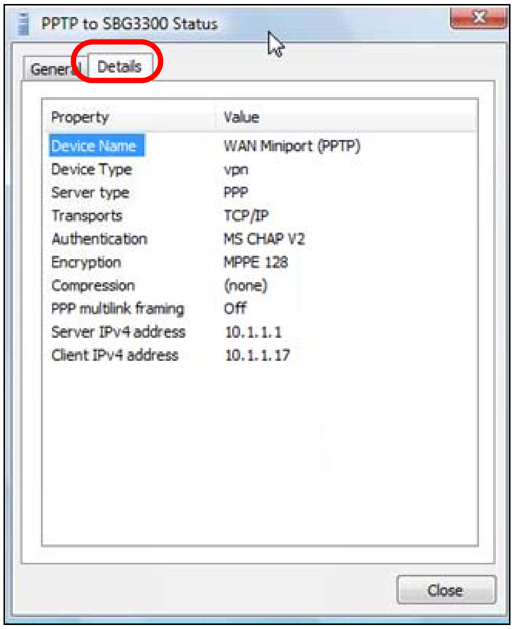
Network 16
Internet access

PPTP to SBG3300
Internet access

Dial-up and VPN

PPTP to SBG3300 **Connected**

17 From the status screen, you can disconnect this connection. Or you can click **Details** to see the connection details. The address 10.1.1.1 and 10.1.1.17 are addresses allocated from the PPTP **IP Address Pool** you configured on the Device (10.1.1.1 - 10.1.1.32).



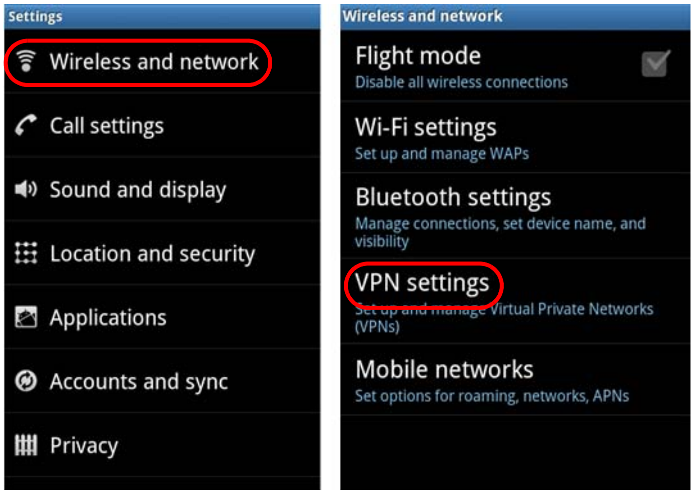
Property	Value
Device Name	WAN Miniport (PPTP)
Device Type	vpn
Server type	PPP
Transports	TCP/IP
Authentication	MS CHAP V2
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Server IPv4 address	10.1.1.1
Client IPv4 address	10.1.1.17

18 Access a server or other network resource on subnet 192.168.1.0 behind the Device to make sure your access works.

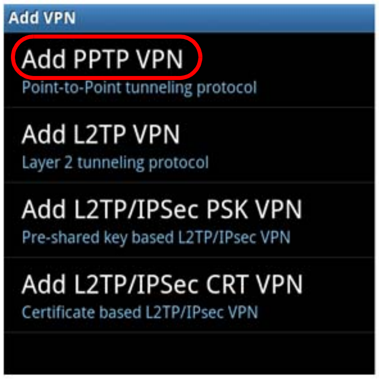
4.14.3 Configuring PPTP VPN on Android Devices (Client)

The following sections cover how to configure the built-in PPTP client in remote user’s Android devices. Due to GUI difference among various Android devices, the figures may not exactly match what your Android device displays. The example settings in these sections match the PPTP VPN configuration example in Section 4.14 on page 69.

1 On your Android device, select **Home** > **Settings** > **Wireless and network** > **VPN settings**.



2 Select **Add VPN** > **Add PPTP VPN**.



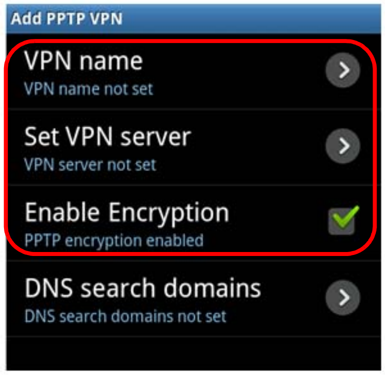
Add VPN

Add PPTP VPN
Point-to-Point tunneling protocol

Add L2TP VPN
Layer 2 tunneling protocol

Add L2TP/IPSec PSK VPN
Pre-shared key based L2TP/IPsec VPN

Add L2TP/IPSec CRT VPN
Certificate based L2TP/IPsec VPN



Add PPTP VPN

VPN name
VPN name not set

Set VPN server
VPN server not set

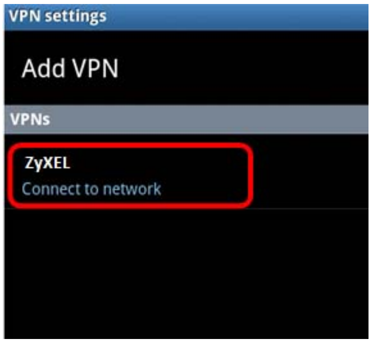
Enable Encryption ☑
PPTP encryption enabled

DNS search domains
DNS search domains not set

3 Fill out the following fields.

- **VPN Name:** Enter a name for your VPN configuration.
- **Set VPN Server:** This is the WAN IP address of the Device, in this example, **172.16.1.2**
- **Enable Encryption:** checked.
- **DNS search domains:** not used.

4 The new configuration will appear on the **VPN settings** screen. You can click the VPN name to begin PPTP connection.



VPN settings

Add VPN

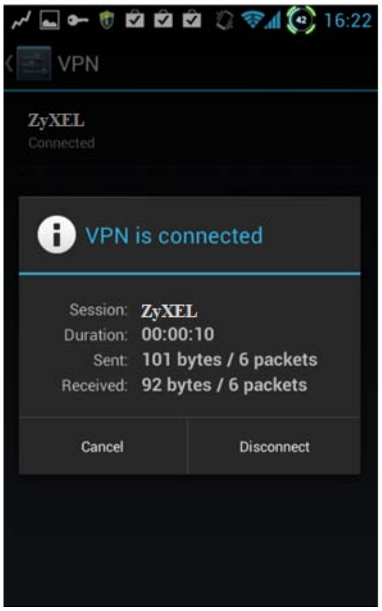
VPNs

ZyXEL
Connect to network

5 Enter the username and password of your user account configured on the Device.

Note: The user account must have been configured in the **Maintenance** > **User Account** screen. Refer to Chapter 29 on page 300.

6 You can see **Connected** when the PPTP VPN connection has been established. Click the connection name to get connection details. There you can also disconnect.



ZyXEL
Connected

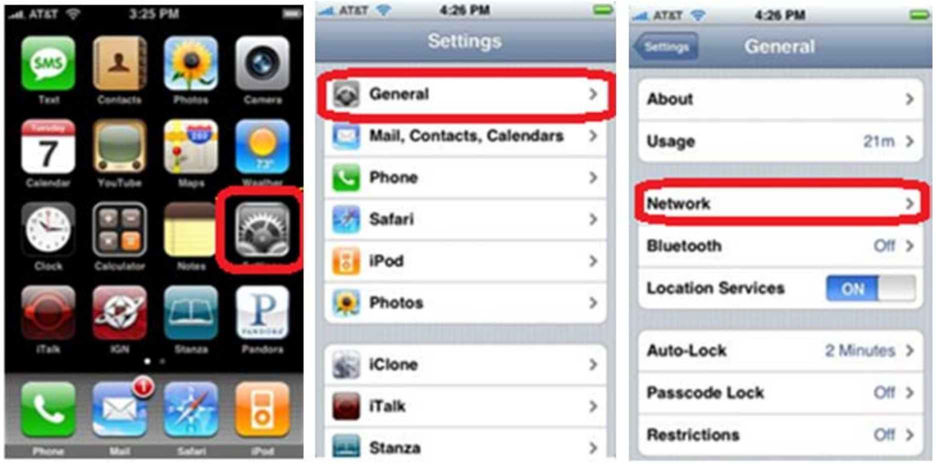
VPN is connected

Session: ZyXEL
Duration: 00:00:10
Sent: 101 bytes / 6 packets
Received: 92 bytes / 6 packets

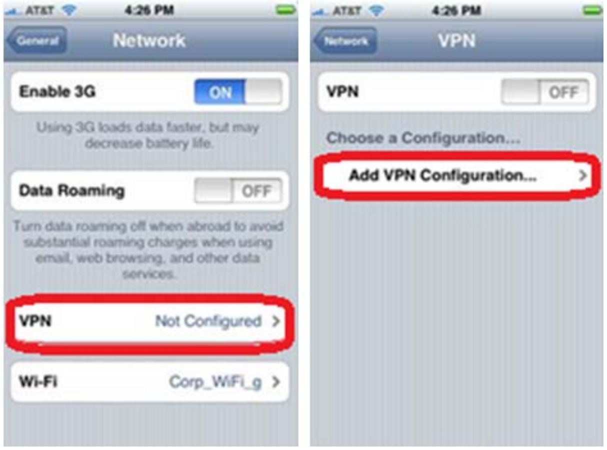
4.14.4 Configuring PPTP VPN in iOS Devices (Client)

The following sections cover how to configure the built-in PPTP client in iOS devices (iPhone, iPad, iPod Touch, etc). Due to GUI difference among various iOS devices, the figures may not match what your iOS device displays. The example settings in these sections match the PPTP VPN configuration example in Section 4.14 on page 69.

1 On your iOS device, select **Home** > **Settings** > **General** > **Network**.



2 Select **VPN** > **Add VPN Configuration…**.



Enable 3G ON

Using 3G loads data faster, but may decrease battery life.

Data Roaming OFF

Turn data roaming off when abroad to avoid substantial roaming charges when using email, web browsing, and other data services.

VPN Not Configured >

Wi-Fi Corp_WiFi_g >

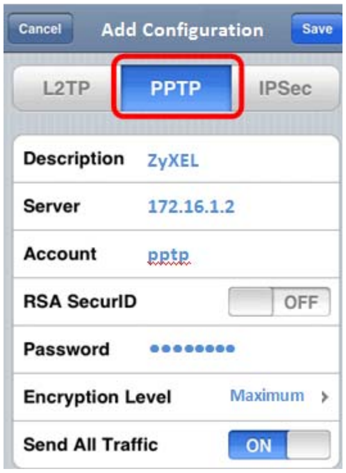
VPN OFF

Choose a Configuration…

Add VPN Configuration… >

3 Select the **PPTP** tab. Enter the following fields.

- **Description:** Enter a name for your VPN configuration.
- **Server:** This is the WAN IP address of the Device, in this example, **172.16.1.2**.
- **Account:** This is the user account created on Device for accessing the network via VPN.
- **RSA SecurID:** Not used in this configuration.
- **Password:** This is the password for account.
- **Secret:** This is your pre-shared key for your VPN connection, in this example, **1234567890**.
- **Send All Traffic:** This example uses the route-all configuration (**ON**).



Description ZyXEL

Server 172.16.1.2

Account pptp

RSA SecurID OFF

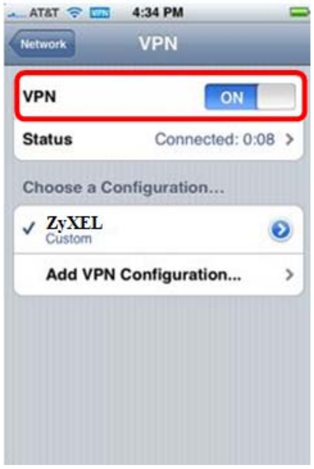
Password ●●●●●●●●●

Encryption Level Maximum >

Send All Traffic ON

4 Save the configuration.

5 The saved configuration will appear on the **VPN** screen. Select it and then slide the VPN bar to the **ON** position. Your iOS device will begin PPTP connection.



VPN ON

Status Connected: 0:08

Choose a Configuration...

✓ ZyXEL Custom

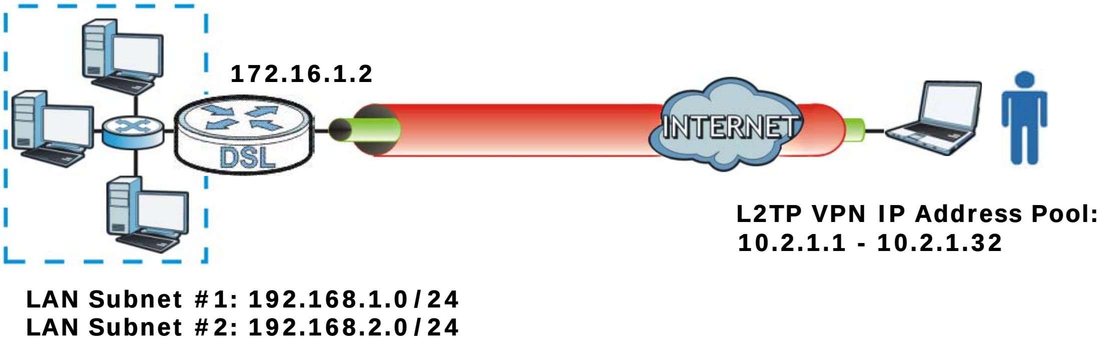
Add VPN Configuration...

4.15 L2TP VPN Tutorial

This section illustrates how to set up a basic L2TP VPN tunnel between the Device and a remote client.

The example uses the following settings in setting up a basic L2TP VPN tunnel.

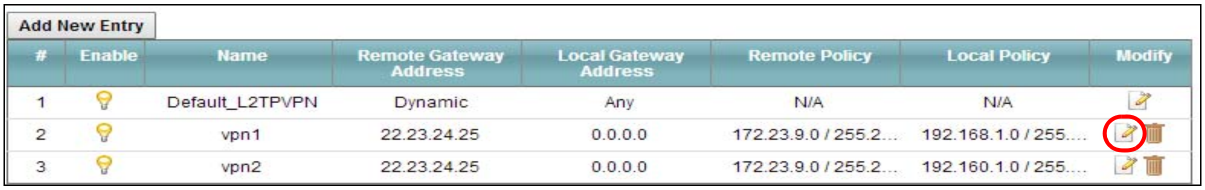
Figure 16 L2TP VPN Example


172.16.1.2
DSL
INTERNET
L2TP VPN IP Address Pool:
10.2.1.1 - 10.2.1.32
LAN Subnet #1: 192.168.1.0/24
LAN Subnet #2: 192.168.2.0/24

- The Device has a static IP address of **172.16.1.2** for the DSL WAN interface.
- The remote user has a dynamic IP address and connects through the Internet.
- Use the default IP address pool to assign the remote users a point-to-point IP addresses from **10.2.1.1** to **10.2.1.32** for use in the L2TP VPN tunnel.
- The access group configuration allows the remote L2TP user to access only the LAN subnet **192.168.2.0/24**.

4.15.1 Configuring the Default_L2TPVPN IPSec VPN Rule (Server)

1 Go to the **VPN** > **IPSec VPN** screen which lists the VPN rules. Click the **Edit** icon of the **Default_L2TPVPN** entry.

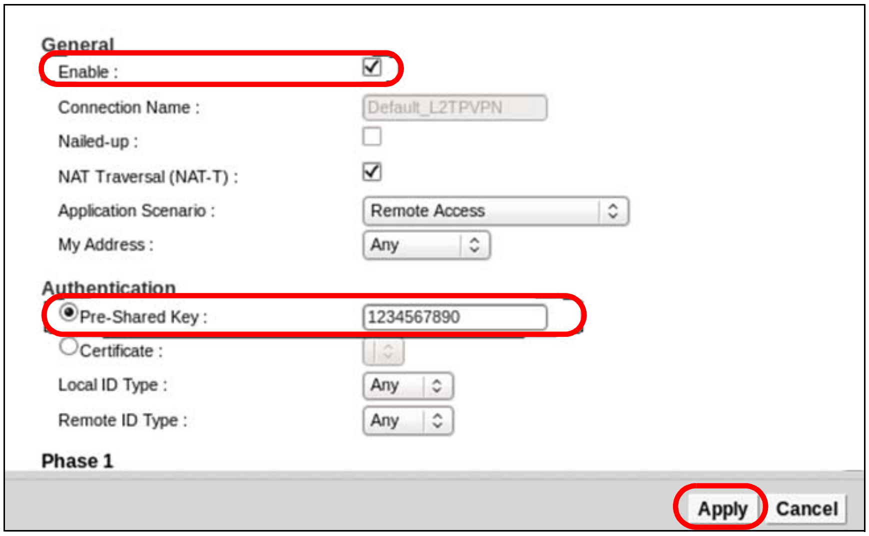


#	Enable	Name	Remote Gateway Address	Local Gateway Address	Remote Policy	Local Policy	Modify
1	💡	Default_L2TPVPN	Dynamic	Any	N/A	N/A	📝
2	💡	vpn1	22.23.24.25	0.0.0.0	172.23.9.0 / 255.2...	192.168.1.0 / 255....	📝 🗑
3	💡	vpn2	22.23.24.25	0.0.0.0	172.23.9.0 / 255.2...	192.160.1.0 / 255....	📝 🗑

2 Select the **Enable** checkbox.

3 Select **Pre-Shared Key** and configure a password. This example uses **1234567890**.

4 Click **Apply**.


General

Enable :	☑
Connection Name :	Default_L2TPVPN
Nailed-up :	□
NAT Traversal (NAT-T) :	☑
Application Scenario :	Remote Access
My Address :	Any

Authentication

● Pre-Shared Key :	1234567890
○ Certificate :	
Local ID Type :	Any
Remote ID Type :	Any

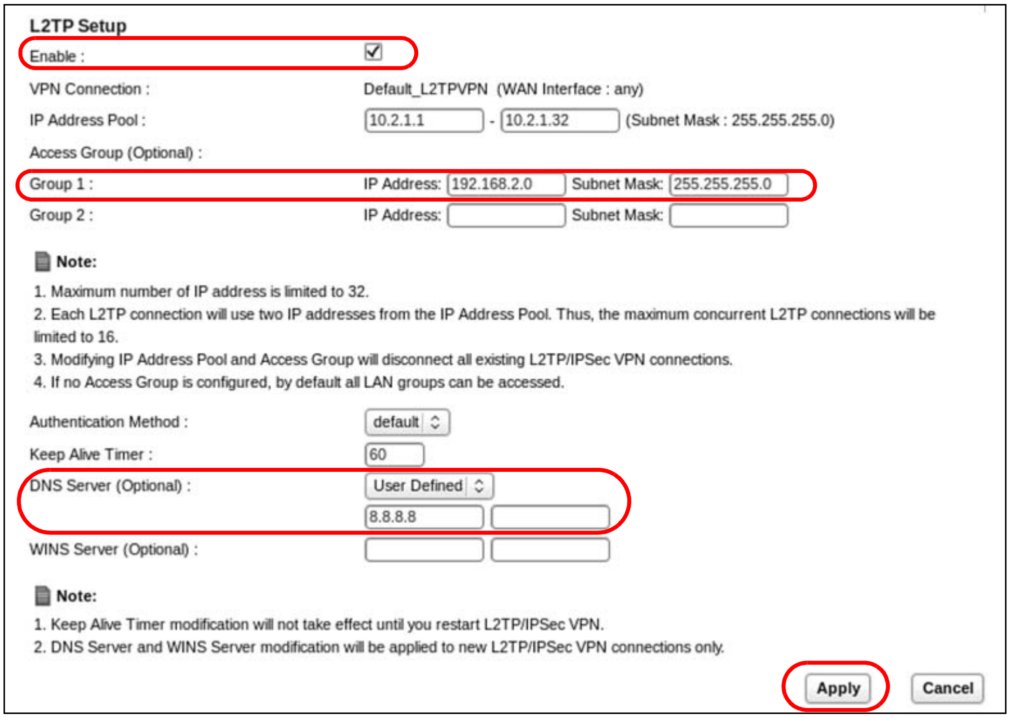
Phase 1

4.15.2 Configuring the L2TP VPN Setup (Server)

1 Go to the **VPN** > **L2TP VPN** > **Setup** screen and configure the following:

- Select the **Enable** checkbox.
- Set **Access Group 1** to **192.168.2.0 / 255.255.255.0**.
- Select **DNS** as **User Defined** and enter a DNS server address. The DNS server address in this example is **8.8.8.8**.

- Click **Apply**.



L2TP Setup

Enable : ☑

VPN Connection : Default_L2TPVPN (WAN Interface : any)

IP Address Pool : 10.2.1.1 - 10.2.1.32 (Subnet Mask : 255.255.255.0)

Access Group (Optional) :

Group 1 : IP Address: 192.168.2.0 Subnet Mask: 255.255.255.0

Group 2 : IP Address: Subnet Mask:

Note:

1. Maximum number of IP address is limited to 32.
2. Each L2TP connection will use two IP addresses from the IP Address Pool. Thus, the maximum concurrent L2TP connections will be limited to 16.
3. Modifying IP Address Pool and Access Group will disconnect all existing L2TP/IPSec VPN connections.
4. If no Access Group is configured, by default all LAN groups can be accessed.

Authentication Method : default

Keep Alive Timer : 60

DNS Server (Optional) : User Defined

8.8.8.8

WINS Server (Optional) :

Note:

1. Keep Alive Timer modification will not take effect until you restart L2TP/IPSec VPN.
2. DNS Server and WINS Server modification will be applied to new L2TP/IPSec VPN connections only.

4.15.3 Configuring L2TP VPN in Windows (Client)

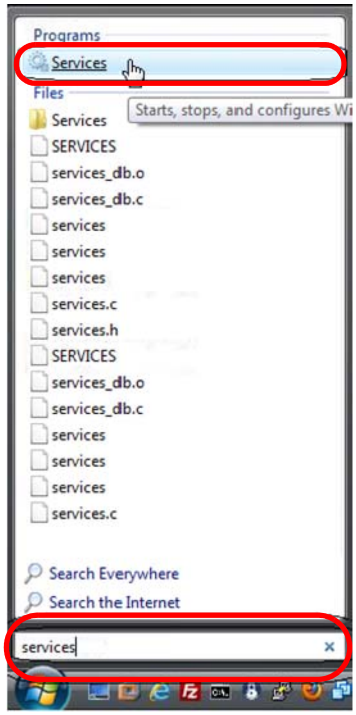
The following sections cover how to configure L2TP on the remote user computers using Windows 7, . The example settings in these sections match the L2TP VPN configuration example in Section on page 81.

4.15.3.1 Enabling IPSec Service in Windows

By default, a Windows computer should have IPSec service enabled. However, before you configure the client, it is suggested to make sure the computer is running the Microsoft IPSec service.

For Windows 7

1 Click the **Start** button and enter “services” in the text box. Then click **Services** under the **Programs** window.



Programs

Services

Starts, stops, and configures Wi

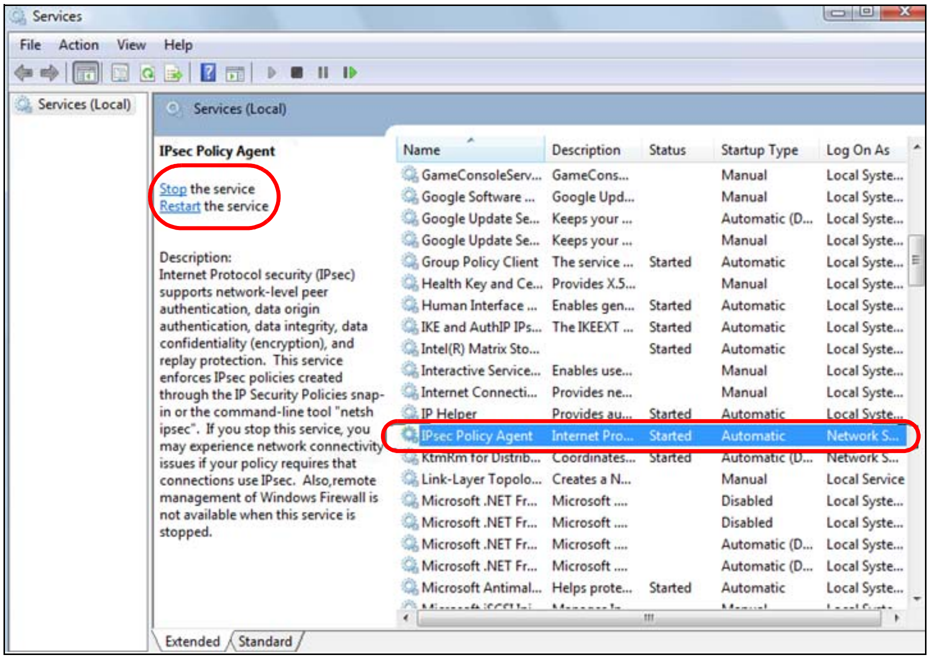
Files

Services
SERVICES
services_db.o
services_db.c
services
services
services
services.c
services.h
SERVICES
services_db.o
services_db.c
services
services
services
services.c

Search Everywhere
Search the Internet

services

2 In the **Services** window, scroll down to find **IPsec Policy Agent**. Make sure the status is **Started**. If not, click **Start the service** in the left panel.



IPsec Policy Agent

Stop the service
Restart the service

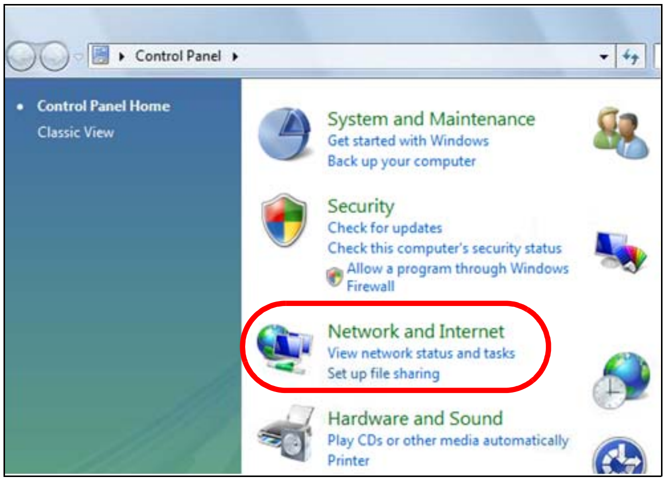
Description:
Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. This service enforces IPsec policies created through the IP Security Policies snap-in or the command-line tool "netsh ipsec". If you stop this service, you may experience network connectivity issues if your policy requires that connections use IPsec. Also,remote management of Windows Firewall is not available when this service is stopped.

Name	Description	Status	Startup Type	Log On As
GameConsoleServ...	GameCons...		Manual	Local Syste...
Google Software ...	Google Upd...		Manual	Local Syste...
Google Update Se...	Keeps your ...		Automatic (D...	Local Syste...
Google Update Se...	Keeps your ...		Manual	Local Syste...
Group Policy Client	The service ...	Started	Automatic	Local Syste...
Health Key and Ce...	Provides X.5...		Manual	Local Syste...
Human Interface ...	Enables gen...	Started	Automatic	Local Syste...
IKE and AuthIP IPs...	The IKEEXT ...	Started	Automatic	Local Syste...
Intel(R) Matrix Sto...		Started	Automatic	Local Syste...
Interactive Service...	Enables use...		Manual	Local Syste...
Internet Connecti...	Provides ne...		Manual	Local Syste...
IP Helper	Provides au...	Started	Automatic	Local Syste...
IPsec Policy Agent	Internet Pro...	Started	Automatic	Network S...
KtmRm for Distrib...	Coordinates...	Started	Automatic (D...	Network S...
Link-Layer Topolo...	Creates a N...		Manual	Local Service
Microsoft .NET Fr...	Microsoft		Disabled	Local Syste...
Microsoft .NET Fr...	Microsoft		Disabled	Local Syste...
Microsoft .NET Fr...	Microsoft		Automatic (D...	Local Syste...
Microsoft .NET Fr...	Microsoft		Automatic (D...	Local Syste...
Microsoft Antimal...	Helps prote...	Started	Automatic	Local Syste...

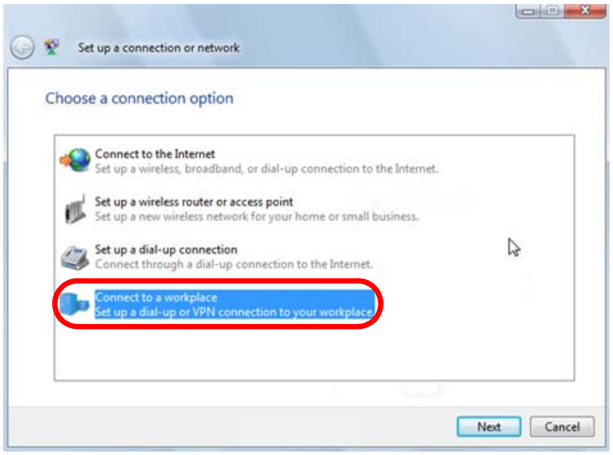
4.15.4 Configuring L2TP VPN on Windows 7

In Windows 7 do the following to establish an L2TP VPN connection.

1 Click **Start** > **Control Panel** > **Network and Internet**.



2 Click **Network and Sharing Center** > **Setup a new connection or network** > **Connect to a workplace**. Click **Next**.


Set up a connection or network

Choose a connection option

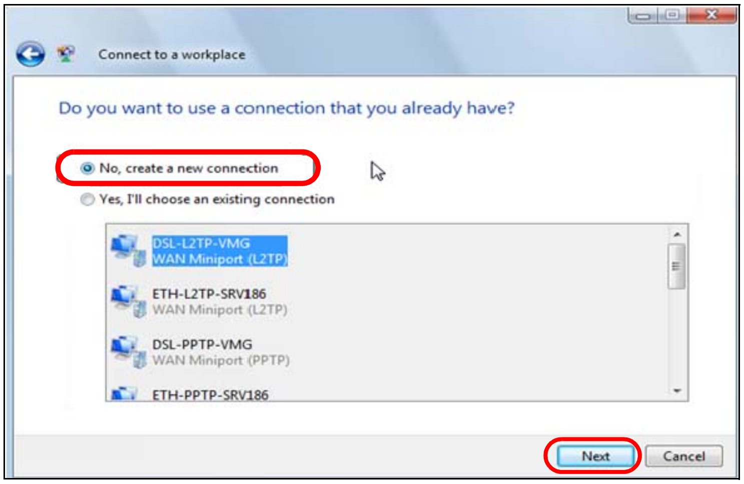
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a wireless router or access point
Set up a new wireless network for your home or small business.

Set up a dial-up connection
Connect through a dial-up connection to the Internet.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

3 Select **No, create a new connection**. Click **Next**.



Connect to a workplace

Do you want to use a connection that you already have?

● No, create a new connection

○ Yes, I'll choose an existing connection

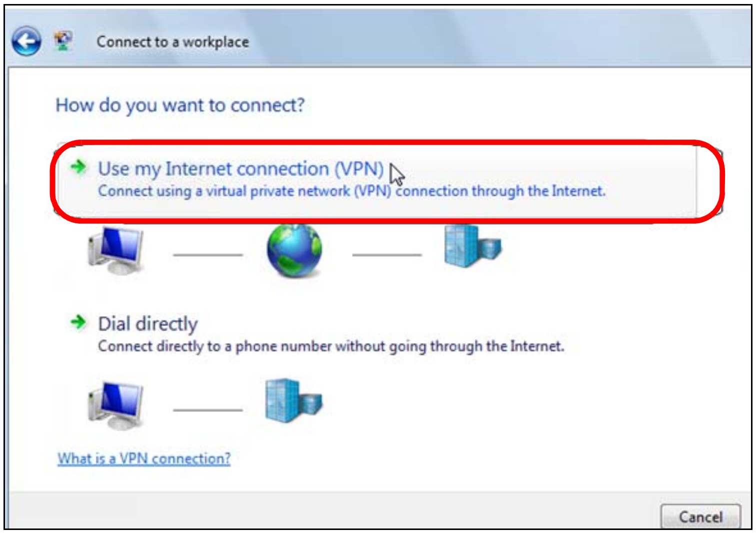
DSL-L2TP-VMG
WAN Miniport (L2TP)

ETH-L2TP-SRV186
WAN Miniport (L2TP)

DSL-PPTP-VMG
WAN Miniport (PPTP)

ETH-PPTP-SRV186

4 Select **Use my Internet connection (VPN)**.



Connect to a workplace

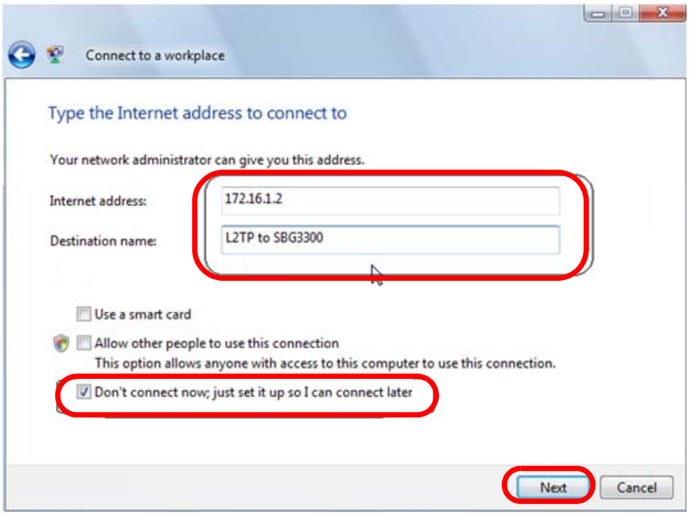
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

5 Enter the domain name or WAN IP Address that you want to connect to (172.16.1.2 in this example) and give this connection a name. Select **Don't connect now; just set it up so I can connect later**. Click **Next**.



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.2

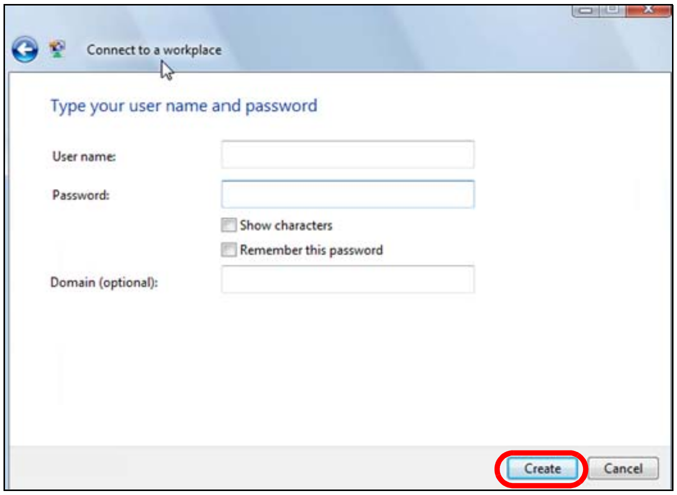
Destination name: L2TP to SBG3300

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

6 Click **Create**. Enter the user name and password later.



Type your user name and password

User name:

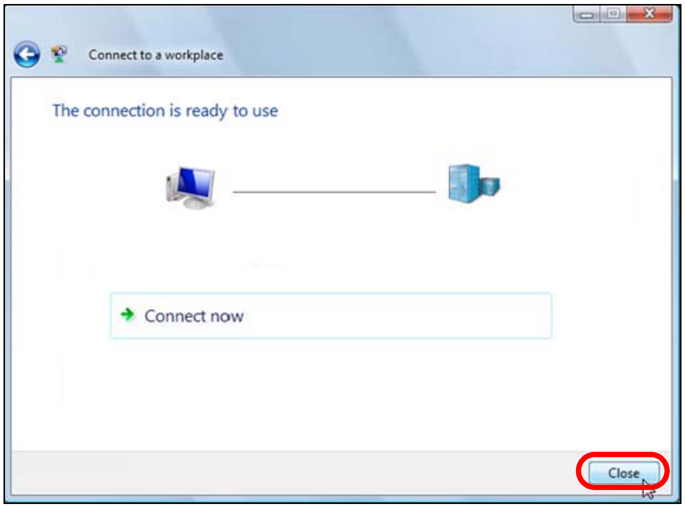
Password:

□ Show characters

□ Remember this password

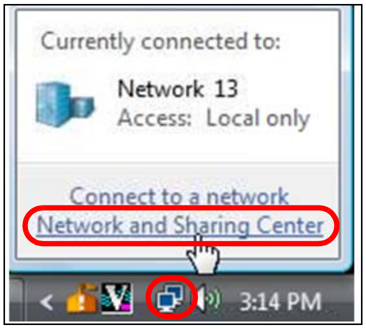
Domain (optional):

7 Click **Close**. Do not connect yet.

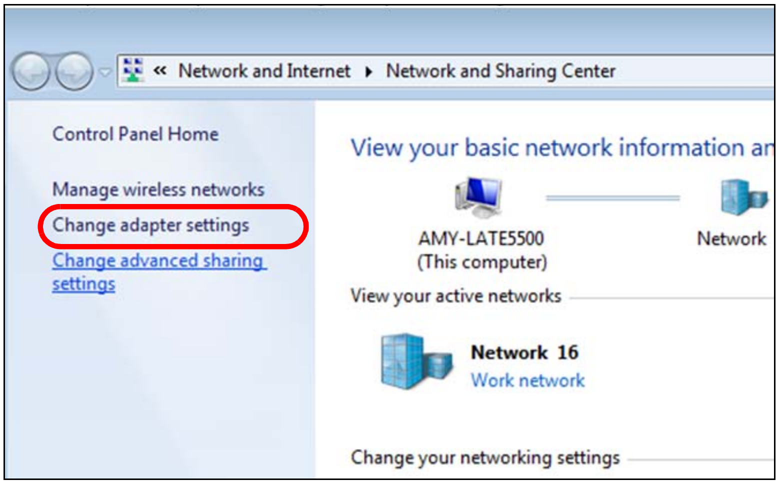


The connection is ready to use

8 Click the **Network** icon in your system tray, then click **Open Network and Sharing Center** .

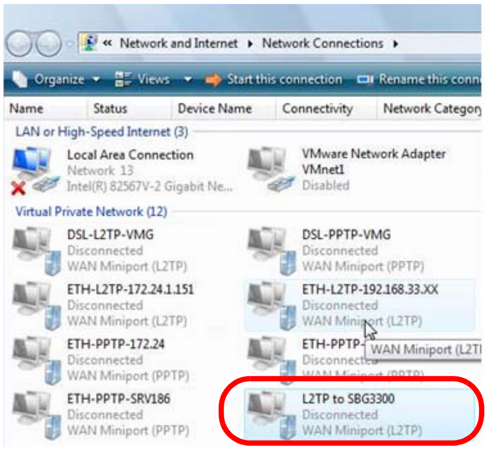


9 Click **Change adapter settings**.


« Network and Internet ▸ Network and Sharing Center
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
AMY-LATE5500
(This computer)
Network
View your active networks
Network 16
Work network
Change your networking settings

View your basic network information ar

10 Double-click the new connection icon.



LAN or High-Speed Internet (3)

Local Area Connection
Network 13
Intel(R) 82567V-2 Gigabit Ne...

VMware Network Adapter VMnet1
Disabled

Virtual Private Network (12)

DSL-L2TP-VMG
Disconnected
WAN Miniport (L2TP)

DSL-PPTP-VMG
Disconnected
WAN Miniport (PPTP)

ETH-L2TP-172.24.1.151
Disconnected
WAN Miniport (L2TP)

ETH-L2TP-192.168.33.XX
Disconnected
WAN Miniport (L2TP)

ETH-PPTP-172.24
Disconnected
WAN Miniport (PPTP)

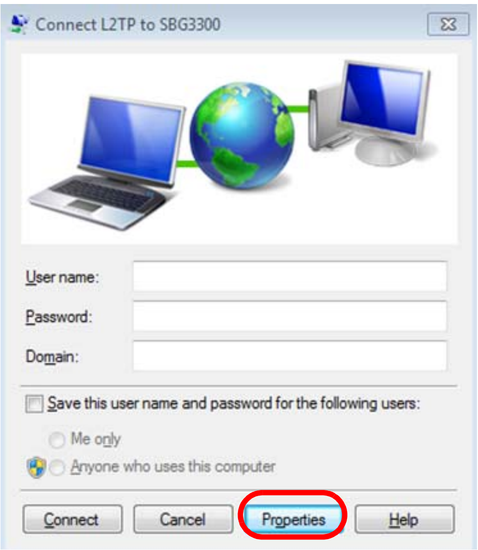
ETH-PPTP-
Disconnect
WAN Miniport (PPTP)

WAN Miniport (L2T

ETH-PPTP-SRV186
Disconnected
WAN Miniport (PPTP)

L2TP to SBG3300
Disconnected
WAN Miniport (L2TP)

11 The connection screen appears. Click **Properties**.


Connect L2TP to SBG3300

User name:

Password:

Domain:

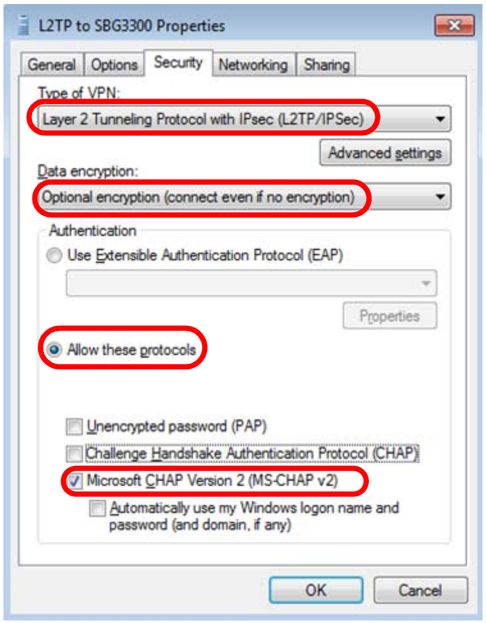
☐ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

12 The **Properties** window appears. Click **Security**.

13 Select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** as the **Type of VPN**. Select the **Optional encryption (connect even if no encryption)** and the **Allow these protocols** radio button. Select **Microsoft CHAP Version 2 (MS-CHAP v2)** and clear all of other check boxes. Do not click **OK** yet.



L2TP to SBG3300 Properties

General | Options | Security | Networking | Sharing

Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Advanced settings

Data encryption:
Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

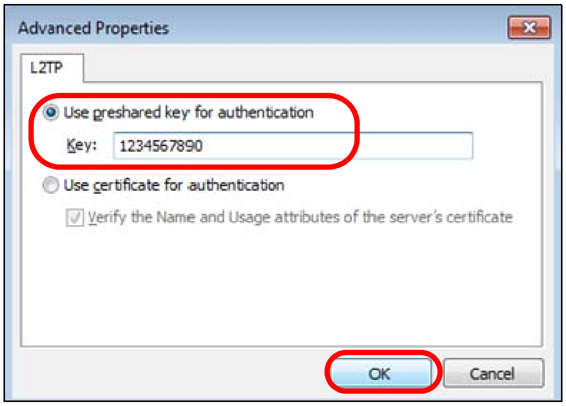
Properties

● Allow these protocols

□ Unencrypted password (PAP)
□ Challenge Handshake Authentication Protocol (CHAP)
☑ Microsoft CHAP Version 2 (MS-CHAP v2)
□ Automatically use my Windows logon name and password (and domain, if any)

OK | Cancel

14 Click **Advanced settings**. Select the **Use preshared key for authentication** radio button. Enter the pre-shared key used in the IPSec configuration that the Device is using for **Default_L2TPVPN** IPSec VPN rule. In this example, enter **1234567890**. Click **OK** to return to the **Connect** window.



Advanced Properties

L2TP

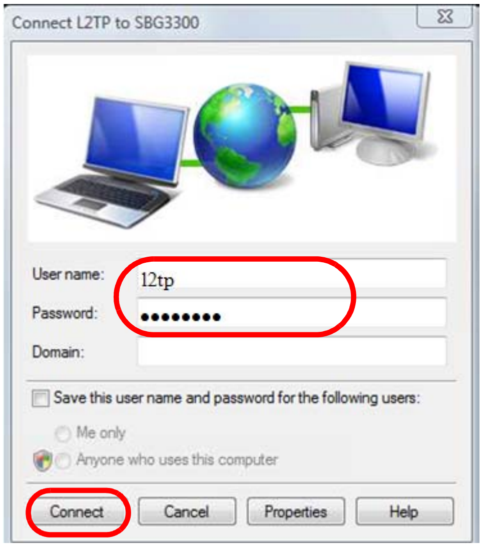
● Use preshared key for authentication
Key: 1234567890

○ Use certificate for authentication
☑ Verify the Name and Usage attributes of the server's certificate

OK | Cancel

15 Enter the username and password of your user account configured on the Device. Click **Connect**.

Note: The user account must have been configured in the **Maintenance** > **User Account** screen. Refer to Chapter 29 on page 300.



Connect L2TP to SBG3300

User name: l2tp

Password: ••••••••

Domain:

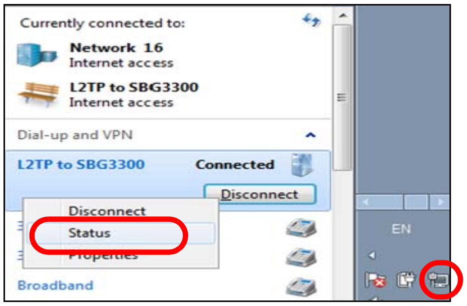
□ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

16 A window appears while the username and password are verified. The connection is then established.

17 Click the **Network** icon in your system tray, then right click the L2TP connection and select **Status** to open the connection status screen.



Currently connected to:

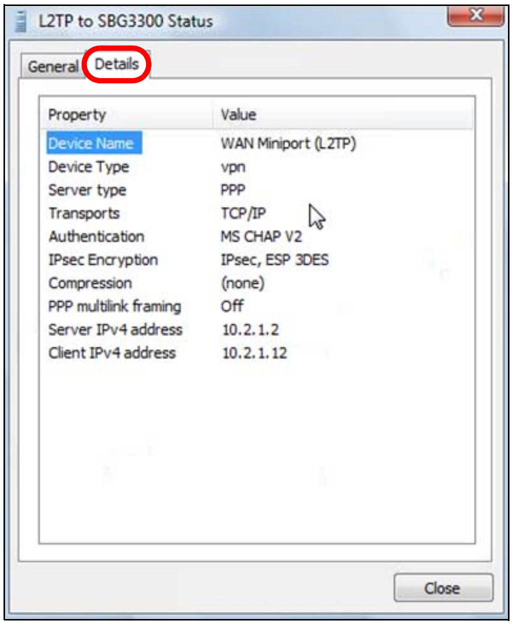
Network 16
Internet access

L2TP to SBG3300
Internet access

Dial-up and VPN

L2TP to SBG3300 Connected

18 From the status screen, you can disconnect this connection. Or you can click **Details** to see the connection details. The address 10.2.1.2 and 10.2.1.12 are addresses allocated from the L2TP **IP Address Pool** you configured on the Device (10.2.1.1 - 10.2.1.32).

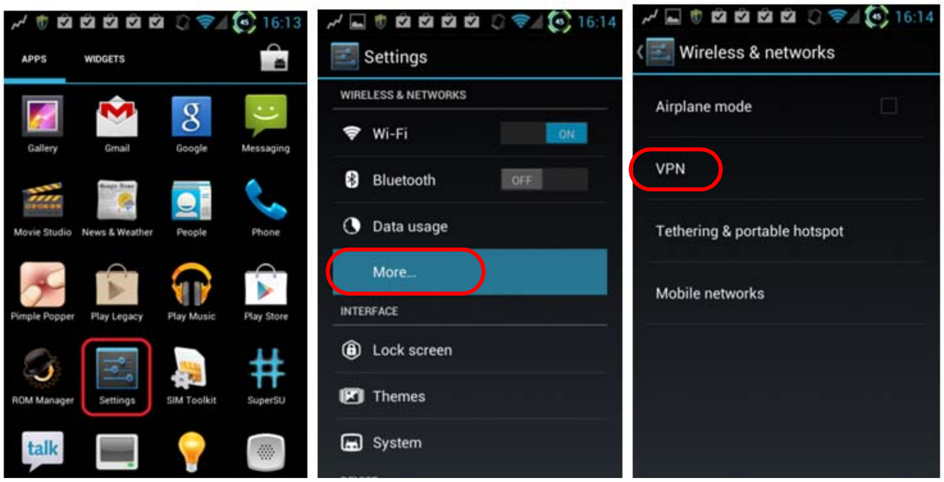


Property	Value
Device Name	WAN Miniport (L2TP)
Device Type	vpn
Server type	PPP
Transports	TCP/IP
Authentication	MS CHAP V2
IPsec Encryption	IPsec, ESP 3DES
Compression	(none)
PPP multilink framing	Off
Server IPv4 address	10.2.1.2
Client IPv4 address	10.2.1.12

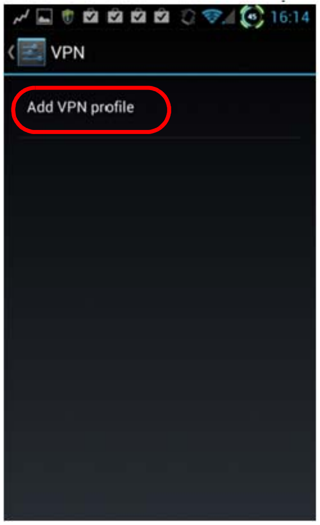
4.15.5 Configuring L2TP VPN on Android Devices (Client)

The following sections cover how to configure the built-in L2TP client in remote user’s Android devices. Due to GUI differences among various Android devices, the figures may not exactly match what your Android device displays. The example settings in these sections match the L2TP VPN configuration example in Section on page 81.

1 On your Android device, select **Home** > **Settings** > **More** > **VPN**.



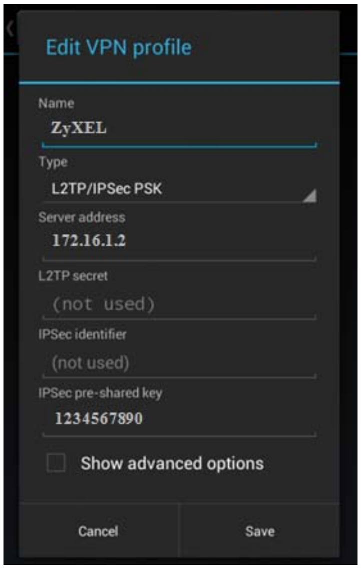
2 Select **Add VPN profile**.



On some Android versions, you may have to tap the + button instead

3 The **Edit VPN profile** screen appears. Fill out the following fields.

- **Name:** Enter a name for your VPN configuration.
- **Type:** Select **L2TP/IPSec PSK**.
- **Server address:** This is the WAN IP address of the Device, in this example, **172.16.1.2**
- **L2TP secret** and **IPSec identifier:** Not used.
- **IPSec pre-shared key:** This is your pre-shared key for your VPN connection, in this example, **1234567890**.



Edit VPN profile

Name
ZyXEL

Type
L2TP/IPSec PSK

Server address
172.16.1.2

L2TP secret
(not used)

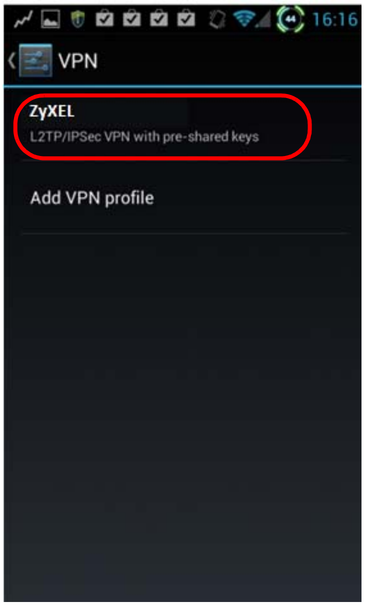
IPSec identifier
(not used)

IPSec pre-shared key
1234567890

□ Show advanced options

4 Save the configuration.

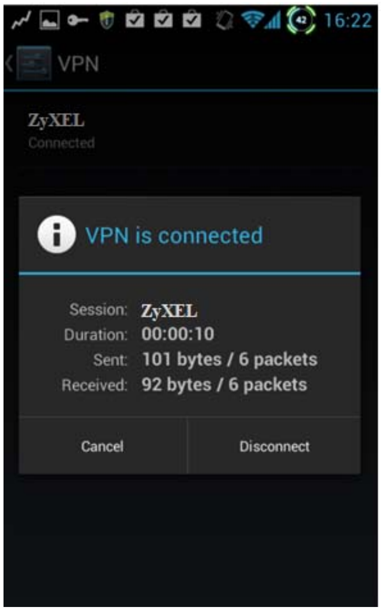
5 The saved configuration appears on the **VPN** screen. Click the VPN name to use the L2TP connection.



6 Enter the username and password of your user account configured on the Device.

Note: The user account must have been configured in the **Maintenance** > **User Account** screen. Refer to Chapter 29 on page 300.

7 You can see **Connected** when the L2TP VPN connection has been established. Click the connection name to get connection details. There you can also disconnect.

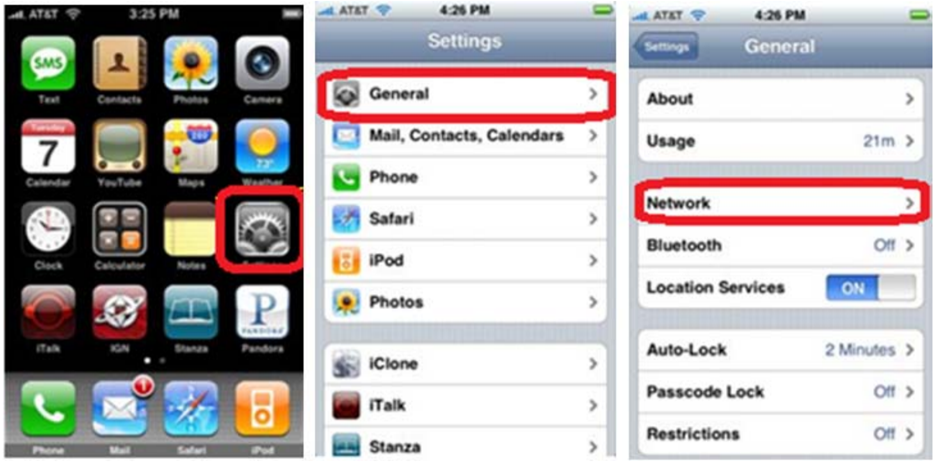


Session: ZyXEL
Duration: 00:00:10
Sent: 101 bytes / 6 packets
Received: 92 bytes / 6 packets

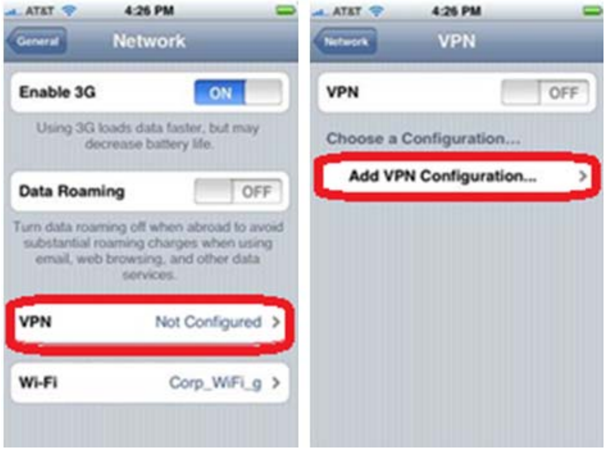
4.15.6 Configuring L2TP VPN in iOS Devices (Client)

The following sections cover how to configure the built-in L2TP client in iOS devices (iPhone, iPad, iPod Touch, etc). Due to GUI difference among various iOS devices, the figures may not match what your iOS device displays. The example settings in these sections matches the L2TP VPN configuration example in Section on page 81.

1 On your iOS device, select **Home** > **Settings** > **General** > **Network**.



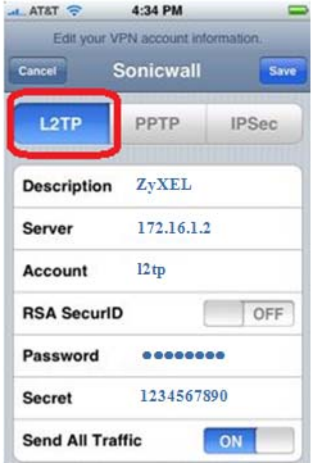
2 Select **VPN** > **Add VPN Configuration...**.


AT&T 4:26 PM
General
Network
Enable 3G ON
Using 3G loads data faster, but may decrease battery life.
Data Roaming OFF
Turn data roaming off when abroad to avoid substantial roaming charges when using email, web browsing, and other data services.
VPN Not Configured
Wi-Fi Corp_WiFi_g
AT&T 4:26 PM
Network
VPN
VPN OFF
Choose a Configuration...
Add VPN Configuration...

3 Select the **L2TP** tab. Enter the following fields.

- **Description:** Enter a name for your VPN configuration.
- **Server:** This is the WAN IP address of the Device, in this example, **172.16.1.2**.
- **Account:** This is the user account created on Device for accessing the network via VPN.
- **RSA SecurID:** Not used in this configuration.
- **Password:** This is the password for account.
- **Secret:** This is your pre-shared key for your VPN connection, in this example, **1234567890**.

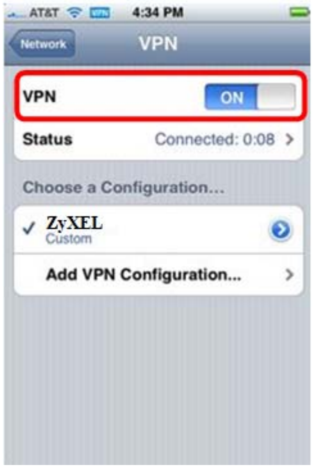
- **Send All Traffic:** This example uses the route-all configuration (**ON**).



Description ZyXEL
Server 172.16.1.2
Account l2tp
RSA SecurID OFF
Password ●●●●●●●●
Secret 1234567890
Send All Traffic ON

4 Save the configuration.

5 The saved configuration appears on the **VPN** screen. Select it and then slide the VPN bar to the **ON** position. Your iOS device will begin L2TP connection.



VPN ON
Status Connected: 0:08
✓ ZyXEL Custom

Part II

Technical Reference

5

Status Screens

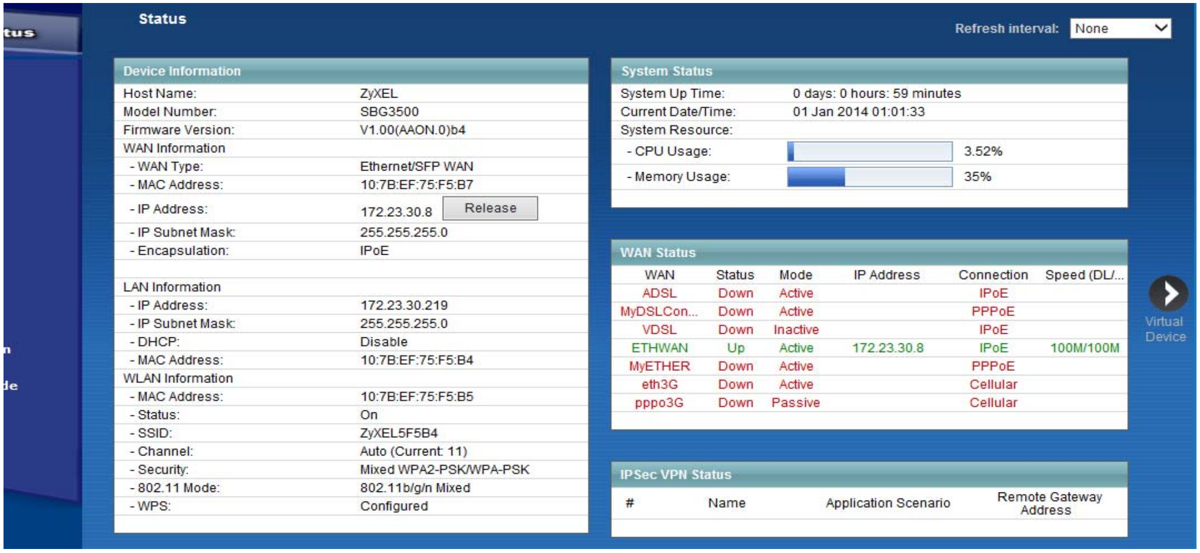
5.1 Overview

After you log into the Web Configurator, the **Status** screen appears. You can use the **Status** screen to look at the current status of the Device, system resources, and interfaces (LAN, WAN, and WLAN).

5.2 The Status Screen

Use this screen to view the status of the Device. Click **Status** to open this screen.

Figure 17 Status Screen



Refresh interval: None

Device Information

Host Name:	ZyXEL
Model Number:	SBG3500
Firmware Version:	V1.00(AAON.0)b4
WAN Information	
- WAN Type:	Ethernet/SFP WAN
- MAC Address:	10:7B:EF:75:F5:B7
- IP Address:	172.23.30.8
- IP Subnet Mask:	255.255.255.0
- Encapsulation:	IPoE
LAN Information	
- IP Address:	172.23.30.219
- IP Subnet Mask:	255.255.255.0
- DHCP:	Disable
- MAC Address:	10:7B:EF:75:F5:B4
WLAN Information	
- MAC Address:	10:7B:EF:75:F5:B5
- Status:	On
- SSID:	ZyXEL5F5B4
- Channel:	Auto (Current: 11)
- Security:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured

System Status

System Up Time:	0 days: 0 hours: 59 minutes
Current Date/Time:	01 Jan 2014 01:01:33
System Resource:	
- CPU Usage:	3.52%
- Memory Usage:	35%

WAN Status

WAN	Status	Mode	IP Address	Connection	Speed (DL/...
ADSL	Down	Active		IPoE	
MyDSLCon...	Down	Active		PPPoE	
VDSL	Down	Inactive		IPoE	
ETHWAN	Up	Active	172.23.30.8	IPoE	100M/100M
MyETHER	Down	Active		PPPoE	
eth3G	Down	Active		Cellular	
pppo3G	Down	Passive		Cellular	

IPSec VPN Status

#	Name	Application Scenario	Remote Gateway Address

Each field is described in the following table.

Table 5 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen.
Device Information	
Host Name	This field displays the Device system name. It is used for identification.
Model Number	This shows the model number of your Device.
Firmware Version	This is the current version of the firmware inside the Device.

Table 5 Status Screen (continued)

LABEL	DESCRIPTION
WAN Information (These fields display when you have a WAN connection.)	
WAN Type	This field displays the current WAN connection type.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your Device.
IP Address	This field displays the current IP address of the Device in the WAN. Click **Release** to release your IP address to 0.0.0.0. If you want to renew your IP address, click **Renew**.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Encapsulation	This field displays the current encapsulation method.
LAN Information	
IP Address	This is the current IP address of the Device in the LAN.
IP Subnet Mask	This is the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the Device is providing to the LAN. Choices are: **Server** - The Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The Device is not providing any DHCP services to the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your Device.
WLAN Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of your Device.
Status	This displays whether WLAN is activated.
SSID	This is the descriptive name used to identify the Device in a wireless LAN.
Channel	This is the channel number used by the Device now.
Security	This displays the type of security mode the Device is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the Device is using in the wireless LAN.
WPS	This displays whether WPS is activated.
Security	
Firewall	This displays the firewall's current security level.
System Status	
System Up Time	This field displays how long the Device has been running since it last started up. The Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Current Date/Time	This field displays the current date and time in the Device. You can change this in **Maintenance> Time Setting**.
System Resource	
CPU Usage	This field displays what percentage of the Device's processing ability is currently used. When this percentage is close to 100%, the Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 10 on page 189).
Memory Usage	This field displays what percentage of the Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the Device is probably becoming unstable, and you should restart the device. See Section 37.2 on page 319, or turn off the device (unplug the power) for a few seconds.

Table 5 Status Screen (continued)

LABEL	DESCRIPTION
WAN Status	
Status	The field displays **Up** when the Device is using the interface and **Down** when the Device is
Mode	The field displays whether the interface is in **Active** or **Passive** mode.
IP Address	The field displays the IP address of the interface.
Connection	The field displays the connection type of the interface.
Speed (DL/UL)	The field displays the speed of the interface's connection.
IPSec VPN Status	
#	This is the VPN policy index number.
Name	This field displays the identification name for the IPSec SA.
Application Scenario	This field displays the scenario type for the IPSec SA.
Remote Gateway Address	This field displays the remote gateway Address used in the SA.

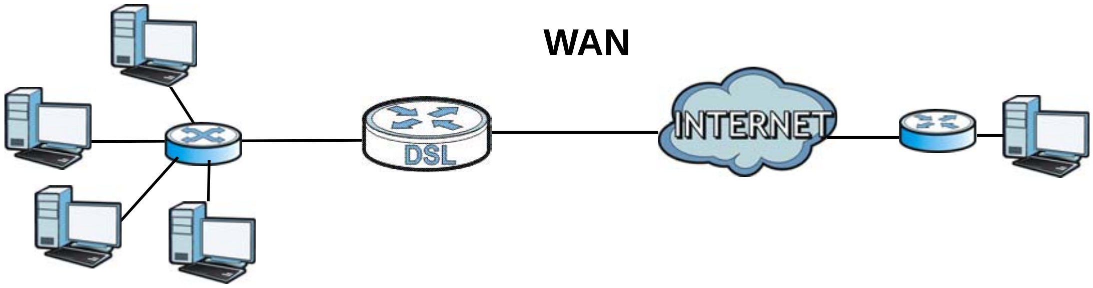
Broadband

6.1 Overview

This chapter discusses the SBG3500-N's **Broadband** screens. Use these screens to configure your SBG3500-N for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

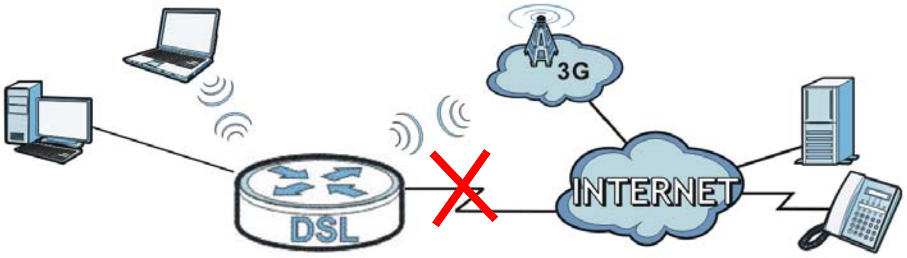
Figure 18 LAN and WAN



3G (third generation) standards for the sending and receiving of voice, video, and data in a mobile environment.

You can attach a 3G wireless adapter to the USB port and set the SBG3500-N to use this 3G connection as your WAN or a backup when the wired WAN connection fails.

Figure 19 3G WAN Connection



6.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the SBG3500-N for Internet access (Section 6.2 on page 106).
- Use the **3G WAN** screen to configure 3G WAN connection (Section 6.3 on page 116).

- Use the **Add New 3G Dongle** screen to view or add a new 3G dongle (Section 6.4 on page 120).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M, and DSL PhyR functions (Section 6.4.1 on page 120).
- Use the **802.1x** screen to view and configure the IEEE 802.1x settings on the SBG3500-N (Section 6.6 on page 122).
- Use the **multi-WAN** screen to configure the multiple WAN load-balancing and fail-over rules to distribute traffic among different interfaces (Section 6.7 on page 124).

Table 6 WAN Setup Overview

LAYER-2 INTERFACE		INTERNET CONNECTION		
CONNECTION	**DSL LINK TYPE**	**MODE**	**ENCAPSULATION**	**CONNECTION SETTINGS**
ADSL/VDSL over PTM	N/A	Routing	PPPoE	PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE	IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	VLAN and QoS
ADSL over ATM	EoA	Routing	PPPoE/PPP0A	ATM PCV configuration, PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE/IPoA	ATM PCV configuration, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	ATM PCV configuration, and QoS
GbE	N/A	Routing	IPoE/PPPoE	PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	VLAN and QoS
3G	N/A	Nailed Up	PPP	Dial string, APN (Access Point Name), IP address, DNS server
		On Demand	PPP	Dial string, APN, Maximum idle time out, DNS server, IP address

6.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the SBG3500-N, which makes it accessible from an outside network. It is used by the SBG3500-N to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the SBG3500-N tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between Finding Out More

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. The SBG3500-N can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.

- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

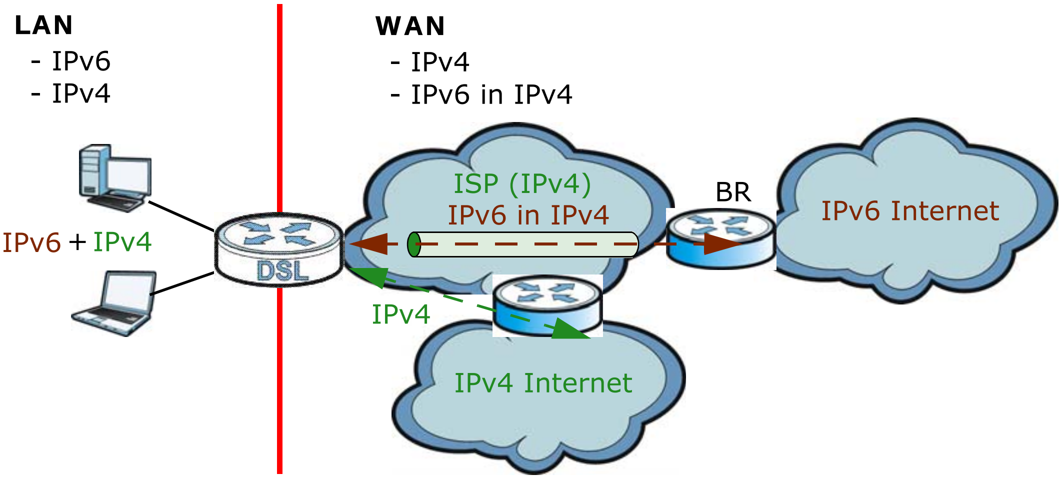
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the SBG3500-N has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The SBG3500-N generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The SBG3500-N uses it's configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 20 IPv6 Rapid Deployment

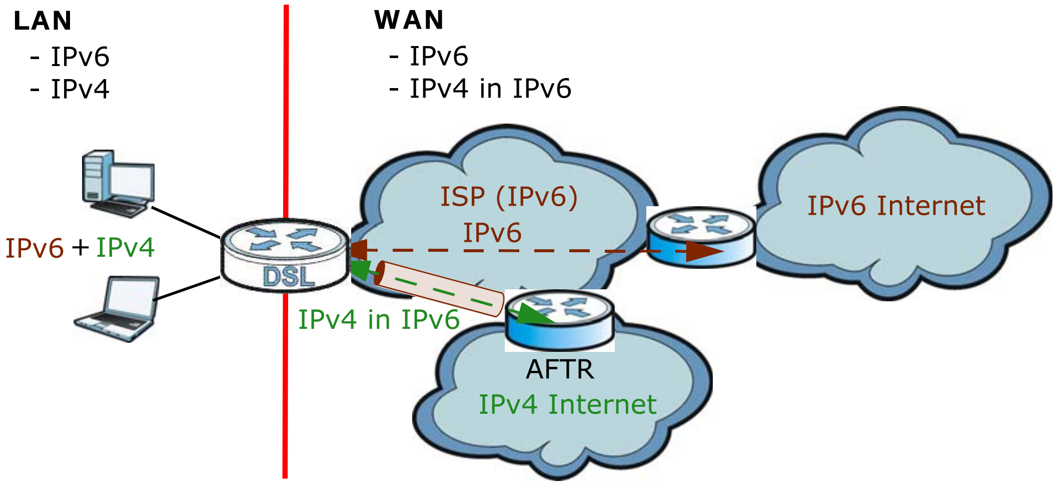


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the SBG3500-N has an IPv6 WAN address and you set **IPv6 / IPv4 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The SBG3500-N tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP’s Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The VDSL Router uses it’s configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 21 Dual Stack Lite



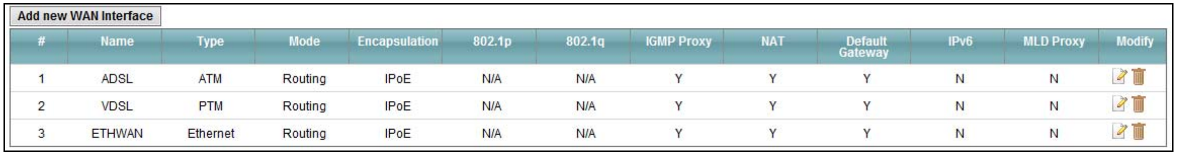
6.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

6.2 The Broadband Screen

Use this screen to change your SBG3500-N’s Internet access settings. Click **Network Setting > Broadband** from the menu. The summary table shows you the configured WAN services (connections) on the SBG3500-N.

Figure 22 Network Setting > Broadband



Add new WAN Interface

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
2	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑
3	ETHWAN	Ethernet	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑

The following table describes the labels in this screen.

Table 7 Network Setting > Broadband

LABEL	DESCRIPTION
Add new WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is an ATM, PTM, or Ethernet connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the SBG3500-N act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the SBG3500-N use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

6.2.1 Add/Edit Internet Connection

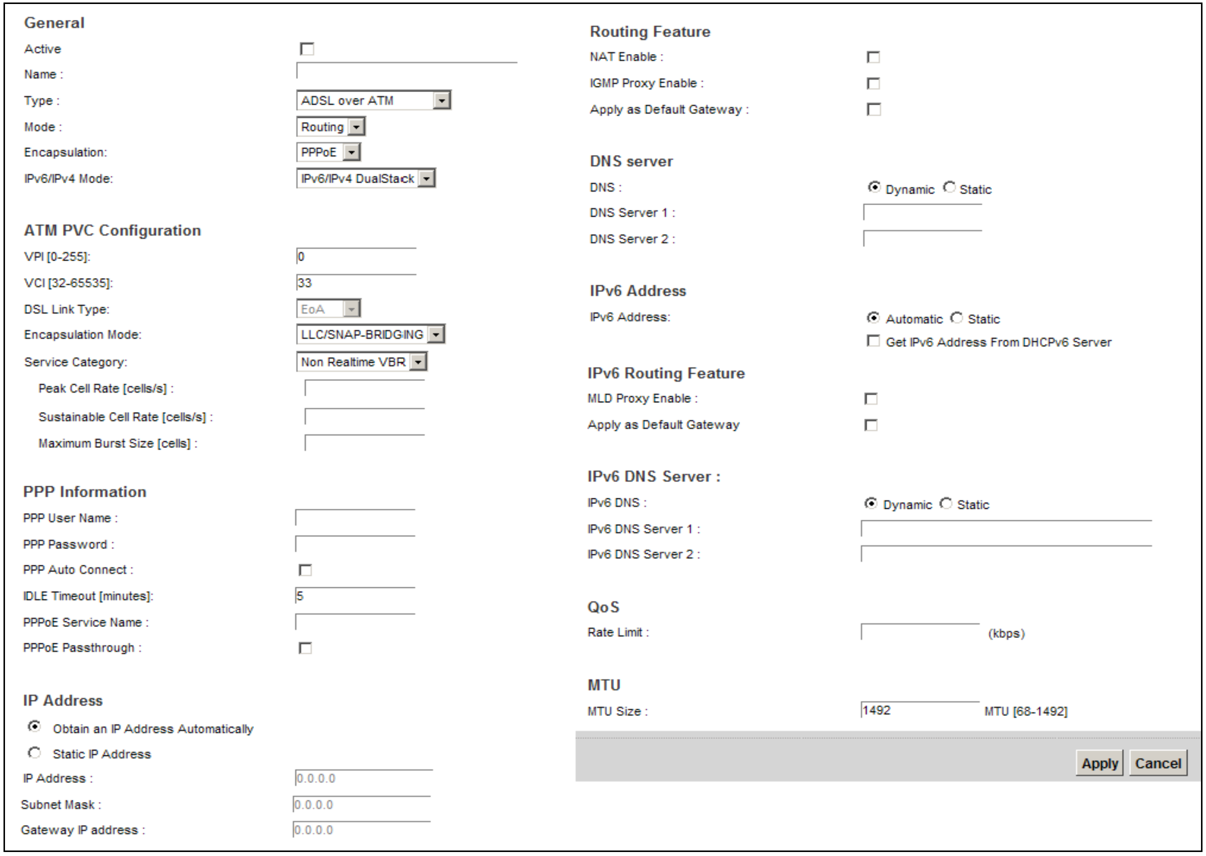
Click **Add new WAN Interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv6/IPv4 mode you select.

6.2.1.1 Routing Mode

Use **Routing** mode if your ISP give you one IP address only and you want multiple computers to share an Internet account.

The following example screen displays when you select the **ADSL over ATM** connection type, **Routing** mode, and **PPPoE** encapsulation. The screen varies when you select other interface type, encapsulation, and IPv6/IPv4 mode.

Figure 23 Routing Mode



General

Active □

Name :

Type : ADSL over ATM

Mode : Routing

Encapsulation: PPPoE

IPv6/IPv4 Mode: IPv6/IPv4 DualStack

ATM PVC Configuration

VPI [0-255]: 0

VCI [32-65535]: 33

DSL Link Type: EoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: Non Realtime VBR

Peak Cell Rate [cells/s] :

Sustainable Cell Rate [cells/s] :

Maximum Burst Size [cells] :

PPP Information

PPP User Name :

PPP Password :

PPP Auto Connect : □

IDLE Timeout [minutes]: 5

PPPoE Service Name :

PPPoE Passthrough : □

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway IP address : 0.0.0.0

Routing Feature

NAT Enable : □

IGMP Proxy Enable : □

Apply as Default Gateway : □

DNS server

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

IPv6 Address

IPv6 Address: ● Automatic ○ Static

□ Get IPv6 Address From DHCPv6 Server

IPv6 Routing Feature

MLD Proxy Enable : □

Apply as Default Gateway □

IPv6 DNS Server :

IPv6 DNS : ● Dynamic ○ Static

IPv6 DNS Server 1 :

IPv6 DNS Server 2 :

QoS

Rate Limit : (kbps)

MTU

MTU Size : 1492 MTU [68-1492]

The following table describes the labels in this screen.

Table 8 Routing Mode

LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.
Name	Specify a descriptive name for this connection.

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
Type	Select whether it is **ADSL/VDSL over PTM**, **ADSL over ATM**, or **Ethernet** connection. • **ADSL/VDSL over PTM**: The SBG3500-N uses the VDSL technology for data transmission over the DSL port. • **ADSL over ATM**: The SBG3500-N uses the ADSL technology for data transmission over the DSL port. • **Ethernet**: The SBG3500-N transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.
Mode	Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. • **PPP over Ethernet (PPPoE)**: PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • **IP over Ethernet (IPoE)**: In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. • **PPP over ATM (PPPoA)**: PPPoA allows just one PPPoA connection over a PVC. • **IP over ATM (IPoA)**: IPoA allows just one RFC 1483 routing connection over a PVC. If your connection type is **ADSL/VDSL over PTM** or **Ethernet**, the choices are **PPPoE** and **IPoE**. If your connection type is **ADSL over ATM**, the choices are **PPPoE**, **PPPoA**, **IPoE** and **IPoA**.
IPv6/IPv4 Mode	Select **IPv4 Only** if you want the Device to run IPv4 only. Select **IPv6/IPv4 DualStack** to allow the Device to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the Device to run IPv6 only.
ATM PVC Configuration (These fields appear when the **Type** is set to **ADSL over ATM**.)	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	This field is not editable. The selection depends on the setting in the **Encapsulation** field. **EoA** (Ethernet over ATM) uses an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods. **PPPoA** (PPP over ATM) allows just one PPPoA connection over a PVC. **IPoA** (IP over ATM) allows just one RFC 1483 routing connection over a PVC.

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **IPoE** or **PPPoE** in the **Select DSL Link Type** field. • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the SBG3500-N needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • **LLC/ENCAPSULATION:** More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Encapsulation** field. • **LLC/SNAP-ROUTING:** In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Encapsulation** field.
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.This field is not available when you select **UBR Without PCR**.
Sustainable Cell Rate	The Sustainable Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
PPP Information	This is available only when you select **PPPoE** or **PPPoA** in the **Mode** field.
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPP Auto Connect	Select this option if you do not want the connection to time out.
IDLE Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not configurable if you select **PPP Auto Connect**.
PPPoE Service Name	Enter the name of your PPPoE service here.

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the SBG3500-N's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the SBG3500-N. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
IP Address	This is available only when you select **IPv4 Only** or **IPv6/IPv4 DualStack** in the **IPv6/IPv4 Mode** field.
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Routing Feature	This is available only when you select **IPv4 Only** or **IPv6/IPv4 DualStack** in the **IPv6/IPv4 Mode** field.
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the SBG3500-N act as an IGMP proxy on this connection. This allows the SBG3500-N to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the SBG3500-N use the WAN interface of this connection as the system default gateway.
DNS Server	This is available only when you select **IPv4 Only** or **IPv6/IPv4 DualStack** in the **IPv6/IPv4 Mode** field.
DNS	Select **Dynamic** if you want the SBG3500-N use the DNS server addresses assigned by your ISP. Select **Static** if you want the SBG3500-N use the DNS server addresses you configure manually.
DNS Server 1	Enter the first DNS server address assigned by the ISP.
DNS Server 2	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This is available only when you select **IPv6/IPv4 DualStack** or **IPv6 Only** in the **IPv6/IPv4 Mode** field.
IPv6 Address	Select **Automatic** if you want to have the SBG3500-N use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address. Select the **Get IPv6 Address From DHCPv6 Server** checkbox if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the SBG3500-N using the IPv6 prefix from an RA. This option is available only when you choose to get your IPv6 address automatically. Select **Static** if you have a fixed IPv6 address assigned by your ISP.

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
WAN IPv6 Address	Enter the IPv6 address assigned by your ISP.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Next Hop	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your SBG3500-N's interface(s). The gateway helps forward packets to their destinations.
IPv6 Routing Feature	You can enable IPv6 routing features in the following section.
MLD Proxy Enable	Select this checkbox to have the SBG3500-N act as an MLD proxy on this connection. This allows the SBG3500-N to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the SBG3500-N use the WAN interface of this connection as the system default gateway.
IPv6 DNS Server	Configure the IPv6 DNS server in the following section.
IPv6 DNS	Select **Dynamic** to have the SBG3500-N get the IPv6 DNS server addresses from the ISP automatically. Select **Static** to have the SBG3500-N use the IPv6 DNS server addresses you configure manually.
IPv6 DNS Server 1	Enter the first IPv6 DNS server address assigned by the ISP.
IPv6 DNS Server 2	Enter the second IPv6 DNS server address assigned by the ISP.
Tunnel	The IPv6 rapid deployment fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 105 for more information.
Enable 6RD	Enable IPv6 rapid deployment to tunnel IPv6 traffic from the local network through the ISP’s IPv4 network.
6RD Type	Select **Static** if you have the IPv4 address of the relay server, otherwise select **DHCP** to have the SBG3500-N detect it automatically through DHCP.
6RD Border Relay Server IP	When you set the **6RD Type** to **Static**, specify the relay server IPv4 address.
6RD IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP’s Border Relay router and connecting to the native IPv6 Internet.
Tunnel	The Dual Stack Lite fields display when you set the **IPv6/IPv4 Mode** field to **IPv6 Only**. Enable Dual Stack Lite to let local computers use IPv4 through an ISP’s IPv6 network. See Dual Stack Lite on page 106 for more information.
Enable DS-Lite	Enable Dual Stack Lite to let local computers use IPv4 through an ISP’s IPv6 network.
DS-Lite Relay Server IP	Specify the transition router’s IPv6 address.
VLAN	These fields appear when the **Type** is set to **ADSL/VDSL over PTM**.
Active	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.

Table 8 Routing Mode (continued)

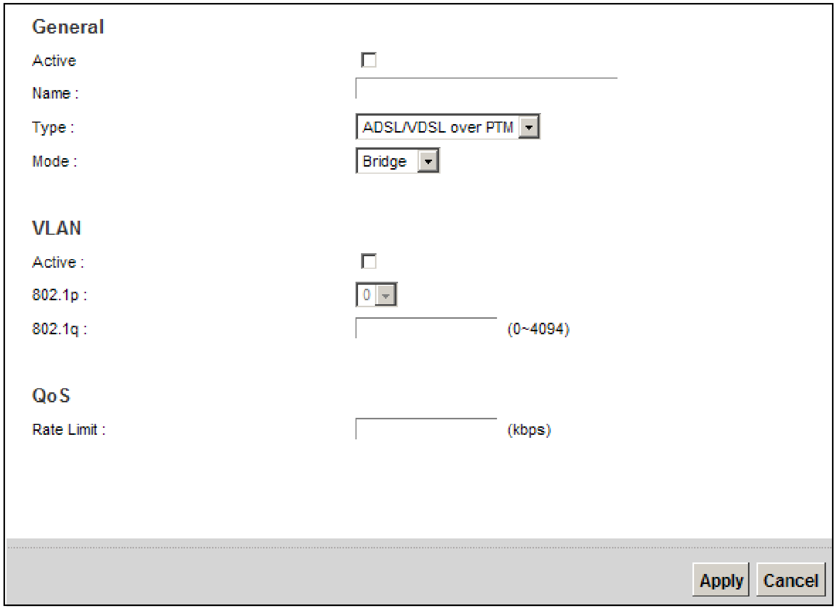
LABEL	DESCRIPTION
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
QoS	
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
MTU	
MTU Size	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to exit this screen without saving.

6.2.1.2 Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode. The screen varies depending on the interface type you select.

If you select **ADSL/VDSL over PTM** as the interface type, the following screen appears.

Figure 24 Bridge Mode (ADSL/VDSL over PTM)



General

Active □

Name :

Type : ADSL/VDSL over PTM

Mode : Bridge

VLAN

Active : □

802.1p : 0

802.1q : (0~4094)

QoS

Rate Limit : (kbps)

The following table describes the fields in this screen.

Table 9 Bridge Mode (ADSL/VDSL over PTM)

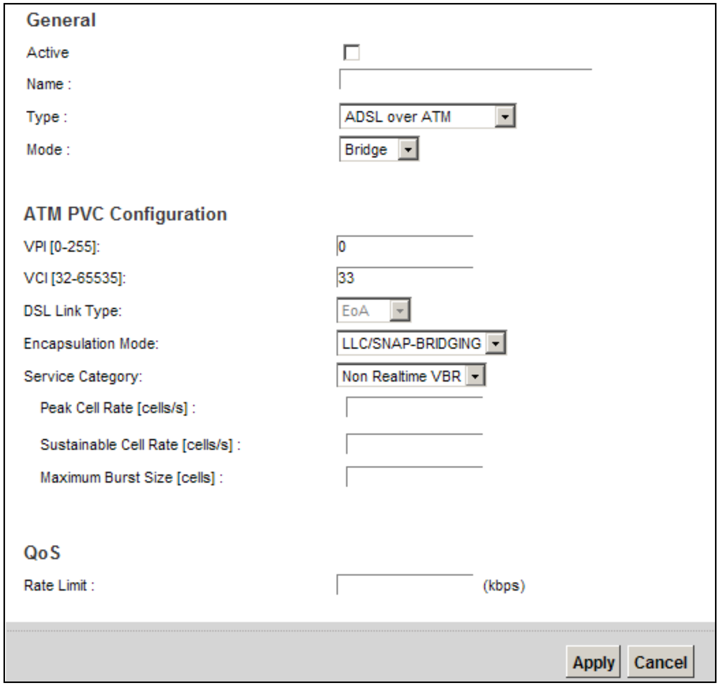
LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.
Name	Enter a service name of the connection.
Type	Select **ADSL/VDSL over PTM** as the interface that you want to configure. The SBG3500-N uses the VDSL technology for data transmission over the DSL port.

Table 9 Bridge Mode (ADSL/VDSL over PTM) (continued)

LABEL	DESCRIPTION
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP’s DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	This section is available only when you select **ADSL/VDSL over PTM** in the **Type** field.
Active	Select this to add the VLAN Tag (specified below) to the outgoing traffic through this connection.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
QoS	
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

If you select **ADSL over ATM** as the interface type, the following screen appears.

Figure 25 Bridge Mode (ADSL over ATM)



General

Active □

Name :

Type : ADSL over ATM

Mode : Bridge

ATM PVC Configuration

VPI [0-255]: 0

VCI [32-65535]: 33

DSL Link Type: EoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: Non Realtime VBR

Peak Cell Rate [cells/s] :

Sustainable Cell Rate [cells/s] :

Maximum Burst Size [cells] :

QoS

Rate Limit : (kbps)

The following table describes the fields in this screen.

Table 10 Bridge Mode (ADSL over ATM)

LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.

Table 10 Bridge Mode (ADSL over ATM) (continued)

LABEL	DESCRIPTION
Name	Enter a service name of the connection.
Type	Select **ADSL over ATM** as the interface for which you want to configure here. The SBG3500-N uses the ADSL technology for data transmission over the DSL port.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP’s DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
ATM PVC Configuration (These fields appear when the **Type** is set to **ADSL over ATM**.)	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	This field is not editable. The selection depends on the setting in the **Encapsulation** field. **EoA** (Ethernet over ATM) uses an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods. **PPPoA** (PPP over ATM) allows just one PPPoA connection over a PVC. **IPoA** (IP over ATM) allows just one RFC 1483 routing connection over a PVC.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **IPoE** or **PPPoE** in the Select DSL Link Type field. • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the SBG3500-N needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • **LLC/ENCAPSULATION:** More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Encapsulation** field. • **LLC/SNAP-ROUTING:** In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Encapsulation** field.
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.This field is not available when you select **UBR Without PCR**.
Sustainable Cell Rate	The Sustainable Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.

Table 10 Bridge Mode (ADSL over ATM) (continued)

LABEL	DESCRIPTION
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
QoS	
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.3 The 3G WAN Screen

Use this screen to configure your 3G settings. Click **Network Setting > Broadband > 3G WAN**.

Note: The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider’s base station, and so on.

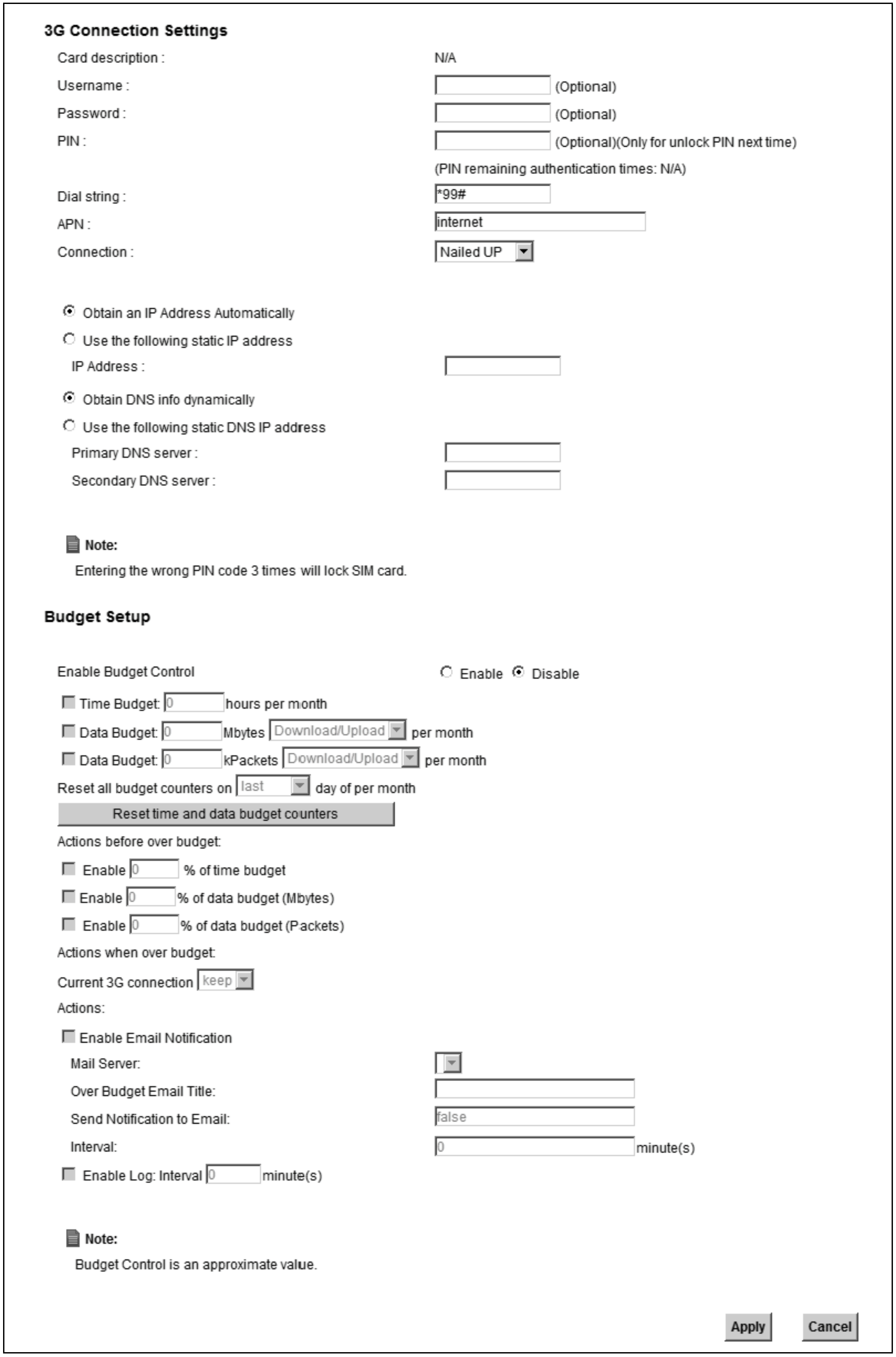


Figure 26 Network Setting **>** Broadband > 3G WAN

3G Connection Settings

Card description : N/A

Username : (Optional)

Password : (Optional)

PIN : (Optional)(Only for unlock PIN next time)

(PIN remaining authentication times: N/A)

Dial string : *99#

APN : internet

Connection : Nailed UP

● Obtain an IP Address Automatically

○ Use the following static IP address

IP Address :

● Obtain DNS info dynamically

○ Use the following static DNS IP address

Primary DNS server :

Secondary DNS server :

Note:

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

Budget Setup

Enable Budget Control ○ Enable ● Disable

□ Time Budget: 0 hours per month

□ Data Budget: 0 Mbytes Download/Upload per month

□ Data Budget: 0 kPackets Download/Upload per month

Reset all budget counters on last day of per month

Reset time and data budget counters

Actions before over budget:

□ Enable 0 % of time budget

□ Enable 0 % of data budget (Mbytes)

□ Enable 0 % of data budget (Packets)

Actions when over budget:

Current 3G connection keep

Actions:

□ Enable Email Notification

Mail Server:

Over Budget Email Title:

Send Notification to Email: false

Interval: 0 minute(s)

□ Enable Log: Interval 0 minute(s)

Note:

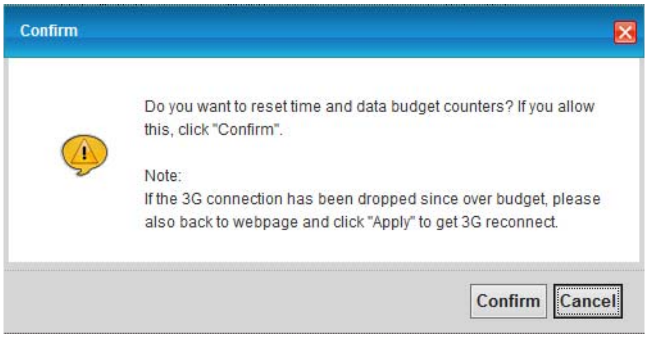
Budget Control is an approximate value.

The following table describes the labels in this screen.

Table 11 Network Setting **>** Broadband > 3G WAN

LABEL	DESCRIPTION
3G Connection Settings	
Card description	This field displays the manufacturer and model name of your 3G card if you inserted one in the SBG3500-N. Otherwise, it displays **N/A**.
Username	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
PIN	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Dial string	Enter the phone number (dial string) used to dial up a connection to your service provider’s base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
APN	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 32 ASCII printable characters. Spaces are allowed.
Connection	Select **Nailed UP** if you do not want the connection to time out. Select **on Demand** if you do not want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the SBG3500-N automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use the following static IP address**.
Obtain DNS info dynamically	Select this to have the SBG3500-N get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the SBG3500-N use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Budget Setup	
Enable Budget Control	Click the radio buttons **Enable** to activate budget control or **Disable** to deactivate budget control.

Table 11 Network Setting **>** Broadband > 3G WAN (continued)

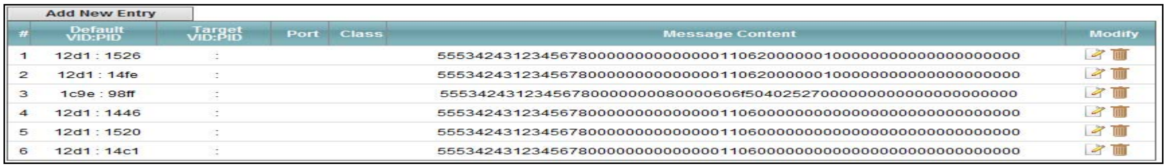
LABEL	DESCRIPTION
Time Budget	Click the check box **Time Budget** to set the number of hours that the user account is allowed per month.
Data Budget	Click the check box **Data Budget** to set the amount of data in **Mbytes** or **kPackets** that is allowed for transmission for the user account. Choose **Upload** or **Download** from the drop-down list to indicate the data stream direction.
Reset Budget	You can choose **Last** or a **Specific** day of the month to reset all budget counters by choosing the options from the drop-down list.
Reset time and data budget counters	Click the **Reset time and data budget coutners** button to reset the counters effective immediately. The below window will appear to prompt you for confirmation. Click **Confirm** for yes and **Cancel** for no.  Confirm Do you want to reset time and data budget counters? If you allow this, click "Confirm". Note: If the 3G connection has been dropped since over budget, please also back to webpage and click "Apply" to get 3G reconnect.
Actions before over budget	
Enable	Click the **Enable** check box and type a number (1-99) in the % box to set the amount of data streams in time, Mbytes and Packets of the data budget.
Actions when over budget	
Current 3G connection	Choose **Keep** or **Drop** from the drop-down list to indicate whether to keep or drop the 3G connection when the data transmission is over the set budget.
Enable Email notification	Click the **Enable Email Notification** check box to active email notification when the data transmission is over the set budget.
Mail Server	Click the mail server IP address from the drop-down list. You need to set the mail server before this step at **Maintenance** > **Email Notification**.
Over budget email title	Type in a string of characters (0-130) for the email title that will be sent when the 3G data transmission usage is over the set budget.
Send notification to email	Type in the email address that corresponds to the mail server you set in **Maintenance** > **Email Notification**.
Interval	Type a number (0-130 characters) for the frequency of the email notifications.
Enable Log	Click the **Enable Log** check box to have the SBG3500-N generate a log report when the 3G data transmission usage is over the set budget. Type a number (0-9999) in the **Minutes** field to indicate the frequency of the log generation.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to return to the previous configuration.

6.4 The Add New 3G Dongle Screen

Use the **Add New 3G Dongle** screen to view and manage the list of 3G dongles the SBG3500-N can use for a 3G backup connection.

Click **Network Setting > Broadband** > **Add New 3G Dongle** to display the following screen.

Figure 27 Network Setting **>** Broadband > Add New 3G Dongle



Add New Entry

#	Default VID:PID	Target VID:PID	Port	Class	Message Content	Modify
1	12d1 : 1526	:			55534243123456780000000000000011062000000100000000000000000000	
2	12d1 : 14fe	:			55534243123456780000000000000011062000000100000000000000000000	
3	1c9e : 98ff	:			55534243123456780000000080000606f50402527000000000000000000000	
4	12d1 : 1446	:			55534243123456780000000000000011060000000000000000000000000000	
5	12d1 : 1520	:			55534243123456780000000000000011060000000000000000000000000000	
6	12d1 : 14c1	:			55534243123456780000000000000011060000000000000000000000000000	

The following table describes the labels in this screen.

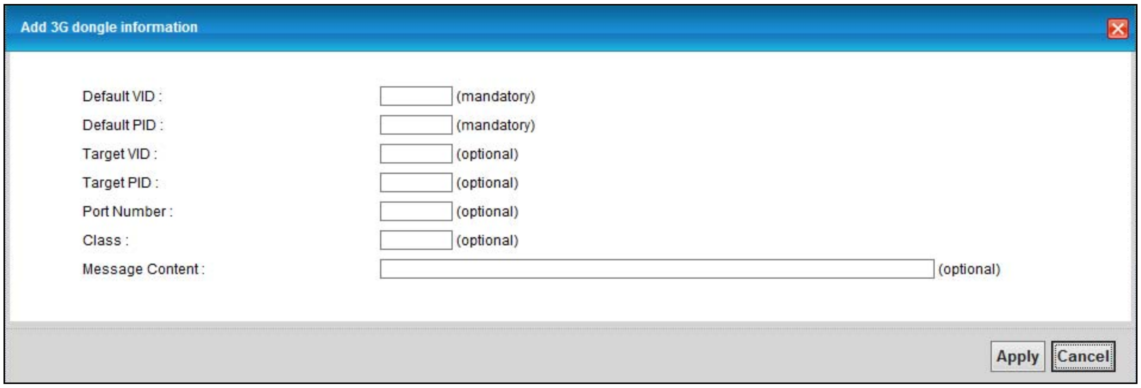
Table 12 Network Setting **>** Network Setting > Add New 3G Dongle

LABEL	DESCRIPTION
Add New Entry	Click this to go to a screen where you can enter information for a new 3G dongle and add it. See Section 6.4.1 on page 120 for more information
#	This is the number of the entry.
Default VID:PID	This is the default vendor ID and product ID of the 3G dongle.
Target VID:PID	This is the target vendor ID and product ID of the 3G dongle.
Port	This is the specified device port of the 3G dongle.
Class	This is the target device class of the 3G dongle.
Message Content	This shows the input message content of the 3G dongle.
Modify	Click the **Edit** icon to modify the information of a 3G dongle. Click the **Delete** icon to remove it.

6.4.1 Add 3G Dongle Information

Click **Add New Entry** in the **Add New 3G Dongle** screen to show the following. Enter the information for a new 3G dongle to add it.

Figure 28 Add 3G Dongle Information



Add 3G dongle information

Default VID :		(mandatory)
Default PID :		(mandatory)
Target VID :		(optional)
Target PID :		(optional)
Port Number :		(optional)
Class :		(optional)
Message Content :		(optional)

The following table describes the labels in this screen.

Table 13 Add 3G Dongle Information

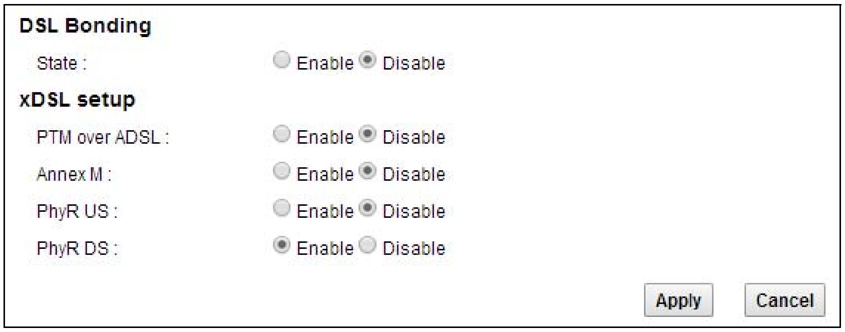
LABEL	DESCRIPTION
Default VID	Enter the default vendor ID of the 3G dongle.
Default PID	Enter the default product ID of the 3G dongle.
Target VID	Enter the target vendor ID of the 3G dongle.
Target PID	Enter the target product ID of the 3G dongle.
Port Number	Enter the specified device port of the 3G dongle.
Class	Enter the target device class of the 3G dongle.
Message Content	Enter the input message content of the 3G dongle.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.5 The Advanced Screen

Use the **Advanced** screen to enable or disable DSL bonding, PTM over ADSL, Annex M, and DSL PhyR functions. The SBG3500-N supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer.

Click **Network Setting > Broadband** > **Advanced** to display the following screen.

Figure 29 Network Setting **>** Broadband > Advanced



DSL Bonding

State : ○ Enable ● Disable

xDSL setup

PTM over ADSL : ○ Enable ● Disable

Annex M : ○ Enable ● Disable

PhyR US : ○ Enable ● Disable

PhyR DS : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 14 Network Setting **>** Network Setting > Advanced

LABEL	DESCRIPTION
State	Select **Enable** to activate DSL bonding state and use both DSL1 and DSL2 ports at the same time to increase data transfer rate.
PTM over ADSL	Select **Enable** to use PTM over ADSL. Since PTM has less overhead than ATM, some ISPs use PTM over ADSL for better performance.
Annex M	You can enable **Annex M** for the SBG3500-N to use double upstream mode to increase the maximum upstream transfer rate.

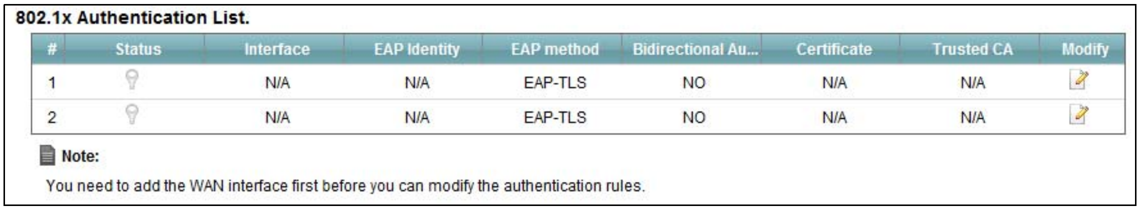
Table 14 Network Setting **>** Network Setting > Advanced (continued)

LABEL	DESCRIPTION
PhyR US	Enable or disable **PhyR US** (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
PhyR DS	Enable or disable **PhyR DS** (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to return to the previous configuration.

6.6 The 802.1x Screen

You can view and configure the 802.1x authentication settings in the **802.1x** screen. Click **Network Setting > Broadband** > **802.1x** to display the following screen.

Figure 30 Network Setting **>** Broadband > 802.1x



802.1x Authentication List.

#	Status	Interface	EAP Identity	EAP method	Bidirectional Au...	Certificate	Trusted CA	Modify
1	💡	N/A	N/A	EAP-TLS	NO	N/A	N/A	✎
2	💡	N/A	N/A	EAP-TLS	NO	N/A	N/A	✎

Note:

You need to add the WAN interface first before you can modify the authentication rules.

The following table describes the labels in this screen.

Table 15 Network Setting **>** Network Setting > 802.1x

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field displays whether the authentication is active or not. A yellow bulb signifies that this authentication is active. A gray bulb signifies that this authentication is not active.
Interface	This is the interface that uses the authentication. This displays **N/A** when there is no interface assigned.
EAP Identity	This shows the EAP identity of the authentication. This displays **N/A** when there is no EAP identity assigned.
EAP method	This shows the EAP method used in the authentication. This displays **N/A** when there is no EAP method assigned.
Bidirectional Authentication	This shows whether bidirectional authentication is allowed.
Certificate	This shows the certificate used for this authentication. This displays **N/A** when there is no certificate assigned.
Trusted CA	This shows the Trusted CA used for this authentication. This displays **N/A** when there is no Trusted CA assigned.

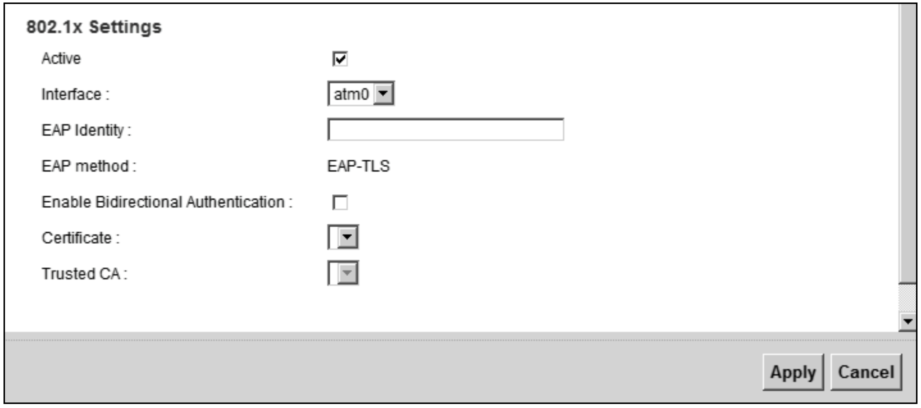
Table 15 Network Setting **>** Network Setting > 802.1x (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to return to the previous configuration.

6.6.1 Edit 802.1x Settings

Use this screen to edit a 802.1x authentication's settings. Click the **Edit** icon next to the rule you want to edit. The screen shown next appears.

Figure 31 802.1x: Add/Edit



802.1x Settings

Active ☑

Interface : atm0

EAP Identity :

EAP method : EAP-TLS

Enable Bidirectional Authentication : □

Certificate :

Trusted CA :

The following table describes the labels in this screen.

Table 16 802.1x: Add/Edit

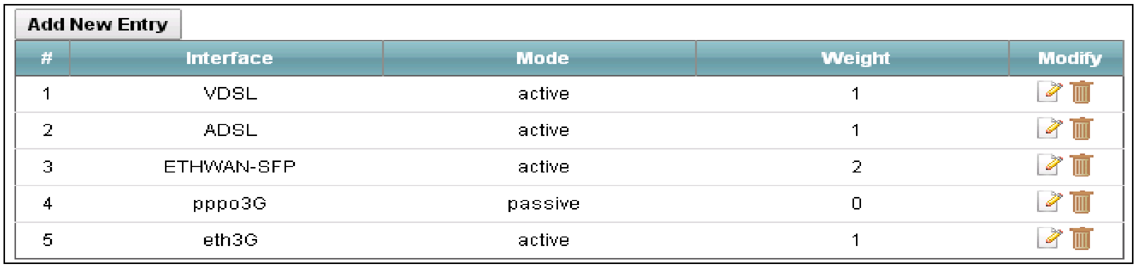
LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate the authentication. Select this to enable the authentication. Clear this to disable this authentication without having to delete the entry.
Interface	Select the interface that uses the authentication.
EAP Identity	Enter the EAP identity of the authentication.
EAP method	This is the EAP method used for this authentication.
Enable Bidirectional Authentication	Select this to allow bidirectional authentication.
Certificate	Select the certificate you want to assign to the authentication. You need to import the certificate in the **Security** > **Certificates** > **Local Certificates** screen.
Trusted CA	Select the Trusted CA you want to assign to the authentication. You need to import the certificate in the **Security** > **Certificates** > **Trusted CA** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.7 The multi-WAN Screen

Use the **multi-WAN** screen to configure the multiple WAN load-balance and fail-over rules to distribute traffic among different interfaces. This helps to increase overall network throughput and reliability. Load-balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

You can only configure one rule for each interface. Click **Network Setting > Broadband** > **multi-WAN** to display the following screen.

Figure 32 Network Setting **>** Broadband > multi-WAN



#	Interface	Mode	Weight	Modify
1	VDSL	active	1	
2	ADSL	active	1	
3	ETHWAN-SFP	active	2	
4	pppo3G	passive	0	
5	eth3G	active	1	

The following table describes the labels in this screen.

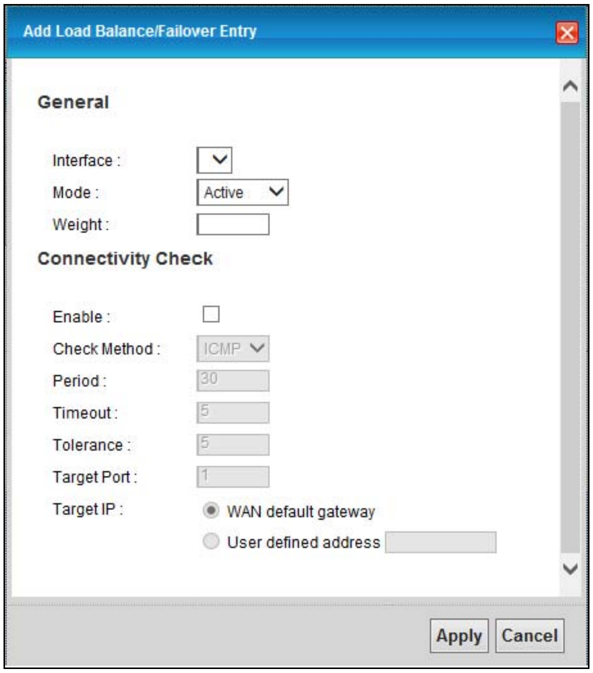
Table 17 Network Setting **>** Network Setting > multi-WAN

LABEL	DESCRIPTION
Add New Entry	Click this button to add a previously removed multi-WAN rule entry. By default, adding new WAN interfaces to the system will generate a corresponding rule entry on this page in active mode with a weight of 1. Each interface can have only one rule. If the interface you want to configure already has a rule, you can edit it, or you can delete it before configuring a new rule.
#	This is the index number of the entry.
Interface	This is the interface that uses the rule.
Mode	This shows whether the rule is **Active** or **Passive**.
Weight	This shows the weight of the rule.
Modify	Click the **Edit** icon to configure the multi-WAN rule. Click the **Delete** icon to remove the multi-WAN rule.

6.7.1 Add/Edit multi-WAN

Click **Add New Entry** in the **multi-WAN** screen or the **Edit** icon next to an existing multi-WAN rule to configure it.

Figure 33 multi-WAN: Add/Edit



Add Load Balance/Failover Entry

General

Interface :

Mode : Active

Weight :

Connectivity Check

Enable : □

Check Method : ICMP

Period : 30

Timeout : 5

Tolerance : 5

Target Port : 1

Target IP : ● WAN default gateway

○ User defined address

The following table describes the labels in this screen.

Table 18 multi-WAN: Add/Edit

LABEL	DESCRIPTION
Interface	If you are adding a new entry, select the interface that you want to configure this rule for. The list shows the interfaces that have not configured multi-WAN rules. If no interface is shown in the list, this means all interfaces already have existing rules. You must delete an old rule before adding a new one.
Mode	Select whether you want to configure the rule as **Active** or **Passive**. If you choose **Active**, the SBG3500-N always attempt to use this connection. If you choose **Passive**, the SBG3500-N only use this connection when all of the connections set to active are down. You can only set one interface to passive mode. Note: The mode of the 3G interface is locked to passive and cannot be changed to active. To set another interface to passive mode, the 3G interface must be deleted first.
Weight	If you choose **Active** in the **Mode** field, specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the SBG3500-N sends through each member interface. The higher an interface’s weight is (relative to the weights of the interfaces), the more traffic the SBG3500-N sends through that interface.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.7.2 How to Configure multi-WAN for Load-Balancing and Fail-Over

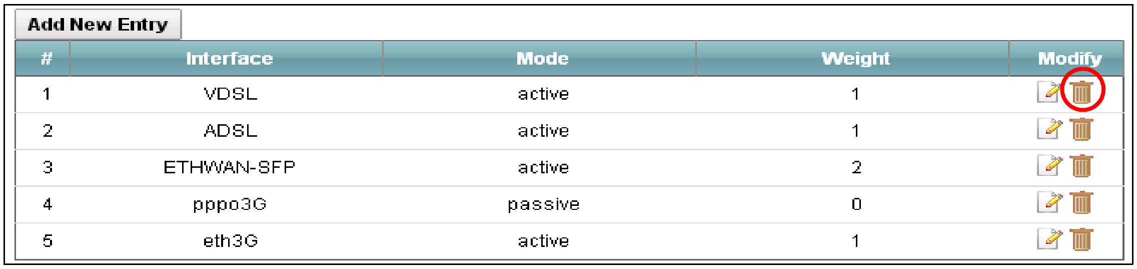
This example shows you how to configure multi-WAN for three WAN connections: an Ethernet WAN connection, an ADSL WAN connection, and a 3G (cellular) WAN connection. The available bandwidth for the Ethernet WAN connection is 3 Mbps, and the available bandwidth for the ADSL WAN connection is 1 Mbps.

As these two wired WAN connections have different bandwidths, you can set multi-WAN to send traffic over these WAN connections in a 3:1 ratio. Most 3G WAN connections charge the user for the amount of data sent, so you can set multi-WAN to send traffic over the 3G WAN connection only if all other WAN connections are unavailable.

6.7.2.1 Configuring multi-WAN

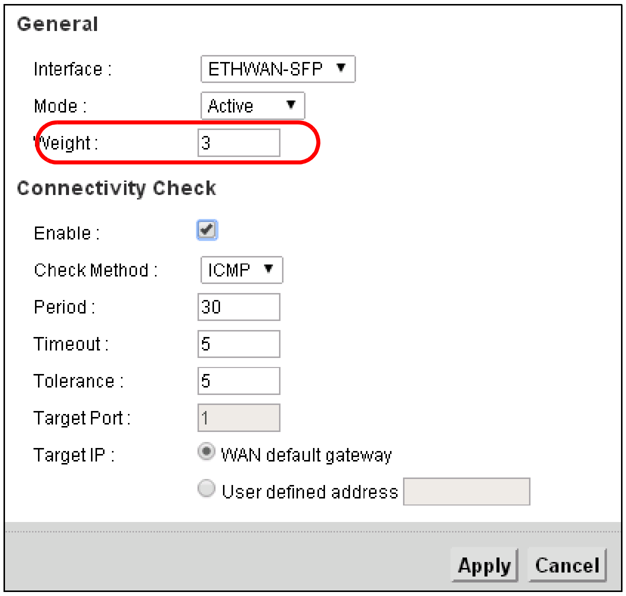
1 Click **Network Setting** > **Broadband** > **multi-WAN**. By default, all available WAN connections on the SBG3500-N are in active mode with a weight of 1, except for the 3G WAN connection which is set to passive mode.

2 Click the **Delete** icon next to the VDSL WAN connection as it is not needed in this example.



#	Interface	Mode	Weight	Modify
1	VDSL	active	1	✎ 🗑
2	ADSL	active	1	✎ 🗑
3	ETHWAN-SFP	active	2	✎ 🗑
4	pppo3G	passive	0	✎ 🗑
5	eth3G	active	1	✎ 🗑

3 Click the **Edit** icon next to the **ETHWAN-SFP** WAN connection. This brings up the edit window. Change the weight field to **3** and click the **Apply** button.

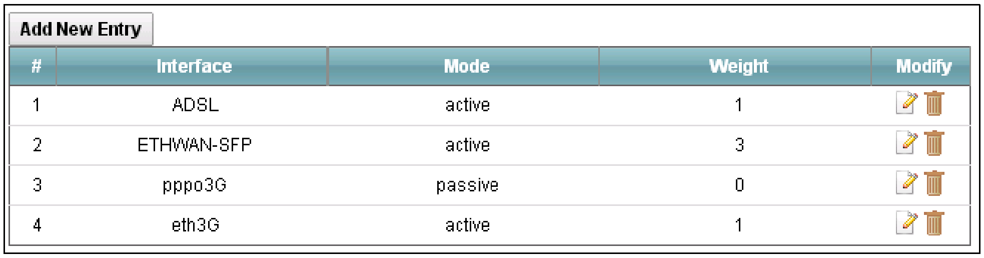

General

Interface :	ETHWAN-SFP ▼
Mode :	Active ▼
Weight :	3

Connectivity Check

Enable :	☑
Check Method :	ICMP ▼
Period :	30
Timeout :	5
Tolerance :	5
Target Port :	1
Target IP :	● WAN default gateway ○ User defined address

4 You have finished the configuration. When both the ETHWAN-SFP and ADSL connections are up, the SBG3500-N will send traffic over these two connections in a 3:1 ratio. When only one of these two connections are up, the SBG3500-N will use that connection exclusively. Only when both of these two connections are down will the SBG3500-N use the 3G connection.



#	Interface	Mode	Weight	Modify
1	ADSL	active	1	
2	ETHWAN-SFP	active	3	
3	pppo3G	passive	0	
4	eth3G	active	1	

6.7.2.2 What Can Go Wrong?

- There can only be one WAN connection configured as passive mode at a time. If there is already a WAN connection configured as passive mode, you will not be able to add or edit another WAN connection in passive mode until the aforementioned WAN connection is changed to active mode or deleted.
- The SBG3500-N will automatically add newly created WAN connections (from the **Network Setting** > **Broadband** > **Broadband** screen) to the multi-WAN configuration as active mode with a weight of 1. If you are creating a new WAN connection for other purposes (such as exclusive VPN use), you will need to delete that WAN connection from the multi-WAN configuration. Deleting a WAN connection from the multi-WAN screen does not delete the WAN connection from the **Broadband** page.
- A WAN connection can only be listed once in the multi-WAN configuration table. If you are trying to add a new entry but do not see the desired WAN connection in the **Interface** drop-down list, it is probably already in the multi-WAN configuration. The **Interface** drop-down list in the **Add/ Edit** screen only includes WAN connections which currently exist on the SBG3500-N but are not currently configured in multi-WAN.

6.8 Technical Reference

The following section contains additional technical information about the SBG3500-N features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The SBG3500-N can work in bridge mode or routing mode. When the SBG3500-N is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over ATM (PPPoA)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The SBG3500-N encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider’s (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the SBG3500-N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the SBG3500-N does that part of the task. Furthermore, with NAT, all of the LANs’ computers will have access.

ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the

4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the SBG3500-N queries all directly connected networks to gather group membership. After that, the SBG3500-N periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The SBG3500-N can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the SBG3500-N’s WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.

- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

7

Wireless

7.1 Overview

This chapter describes the Device's **Network Setting > Wireless** screens. Use these screens to set up your Device's wireless connection.

7.1.1 What You Can Do in this Chapter

This section describes the Device's **Wireless** screens. Use these screens to set up your Device's wireless connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 7.2 on page 133).
- Use the **More AP** screen to set up multiple wireless networks on your Device (Section 7.3 on page 140).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Device (Section 7.4 on page 143).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 7.5 on page 144).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 7.6 on page 145).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold (Section 7.7 on page 146).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results (Section 7.8 on page 148).

7.1.2 What You Need to Know

Wireless Basics

“Wireless” is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See Section 7.9 on page 148 for advanced technical information on wireless networks.

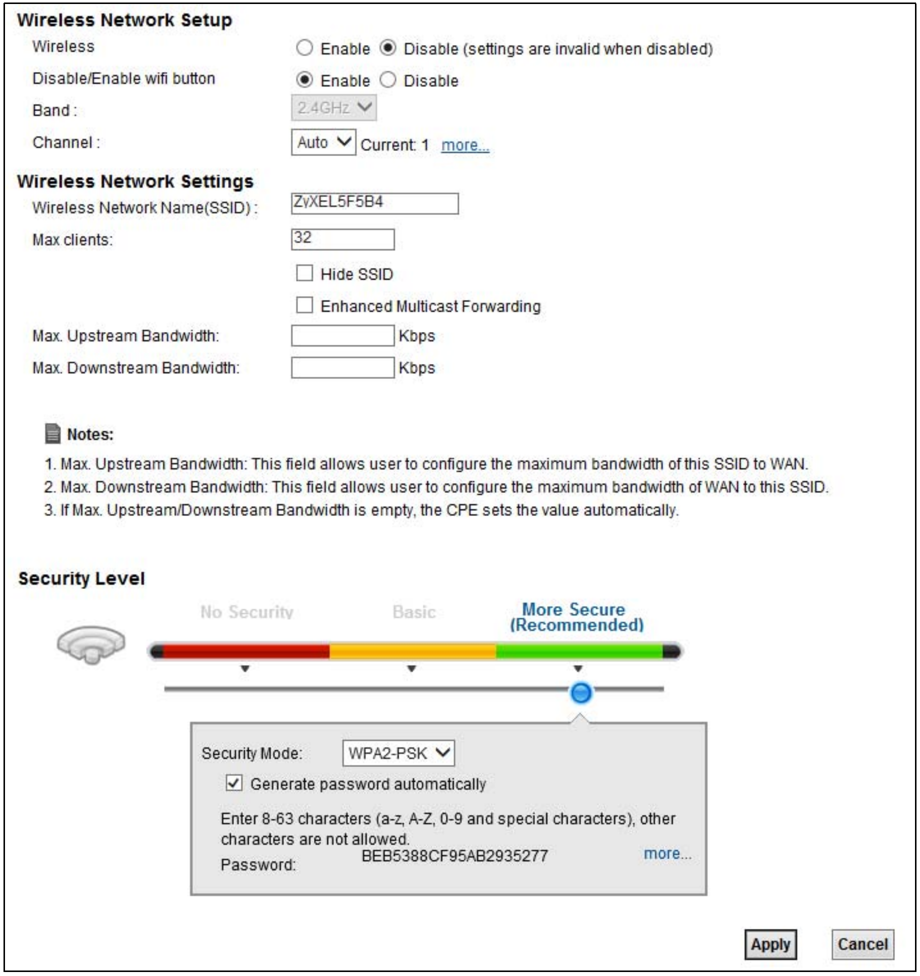
7.2 The General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the Device from a computer connected to the wireless LAN and you change the Device’s SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Device’s new settings.

Click **Network Setting** > **Wireless** to open the **General** screen.

Figure 34 Network Setting > Wireless > General



Wireless Network Setup

Wireless	○ Enable ● Disable (settings are invalid when disabled)
Disable/Enable wifi button	● Enable ○ Disable
Band :	2.4GHz
Channel :	Auto Current: 1 more...

Wireless Network Settings

Wireless Network Name(SSID) :	ZyXEL5F5B4
Max clients:	32
	□ Hide SSID
	□ Enhanced Multicast Forwarding
Max. Upstream Bandwidth:	Kbps
Max. Downstream Bandwidth:	Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

Security Level

Security Mode: WPA2-PSK

☑ Generate password automatically

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

Password: BEB5388CF95AB2935277

The following table describes the general wireless LAN labels in this screen.

Table 19 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can **Enable** or **Disable** the wireless LAN in this field.
Band	This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n wireless clients.
Channel	Set the channel depending on your particular region. Select a channel or use **Auto** to have the Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the Device is currently using then displays next to this field.
more.../less	Click **more...** to show more information. Click **less** to hide them.

Table 19 Network Setting > Wireless > General (continued)

LABEL	DESCRIPTION
Bandwidth	Select whether the Device uses a wireless channel width of **20MHz** or **40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Passphrase Type	If you set security for the wireless LAN and have the Device generate a password, the setting in this field determines how the Device generates the password. Select **None** to set the Device’s password generation to not be based on a passphrase. Select **Fixed** to use a 16 character passphrase for generating a password. Select **Variable** to use a 16 to 63 character passphrase for generating a password.
Passphrase Key	For a fixed type passphrase enter 16 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. For a variable type passphrase enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other through the Device.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the Device. Select both **Client Isolation** and **MBSSID/LAN Isolation** to allow this SSID’s wireless clients to only connect to the Internet through the Device.
Enhanced Multicast Forwarding	Select this check box to allow the Device to convert wireless multicast traffic into wireless unicast traffic.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Maximum Bandwidth	Specify the maximum rate for wireless traffic in kilobits per second (Kbps).
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.

Table 19 Network Setting > Wireless > General (continued)

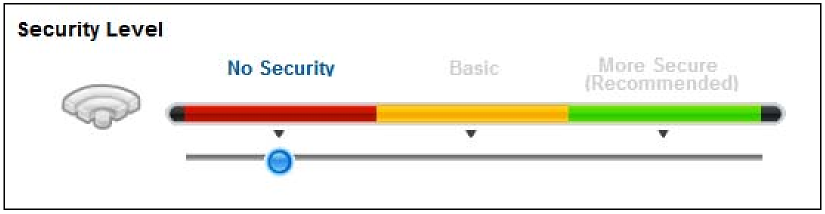
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your Device, your network is accessible to any wireless networking device that is within range.

Figure 35 Wireless > General: No Security



The following table describes the labels in this screen.

Table 20 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all wireless connections without data encryption or authentication.

7.2.2 Basic (WEP Encryption)

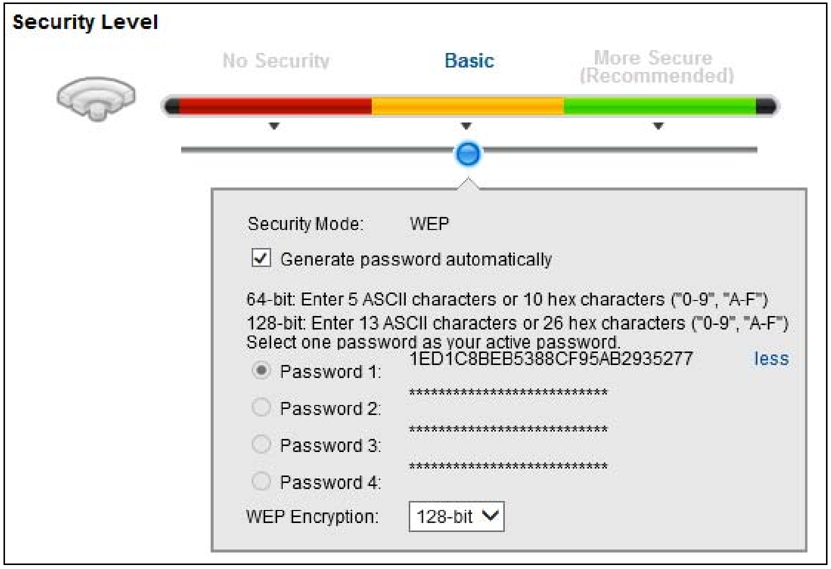
WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it, or use WPA or WPA2 if your wireless devices support it and you have a RADIUS server. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

Your Device allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption, click **Network Setting** > **Wireless** to display the **General** screen, then select **Basic** as the security level.

Figure 36 Wireless > General: Basic (WEP)



Security Mode: WEP

☑ Generate password automatically

64-bit: Enter 5 ASCII characters or 10 hex characters ("0-9", "A-F")
128-bit: Enter 13 ASCII characters or 26 hex characters ("0-9", "A-F")
Select one password as your active password.

● Password 1: 1ED1C8BEB5388CF95AB2935277 less
○ Password 2: ****************************
○ Password 3: ****************************
○ Password 4: ****************************

WEP Encryption: 128-bit

The following table describes the labels in this screen.

Table 21 Wireless > General: Basic (WEP)

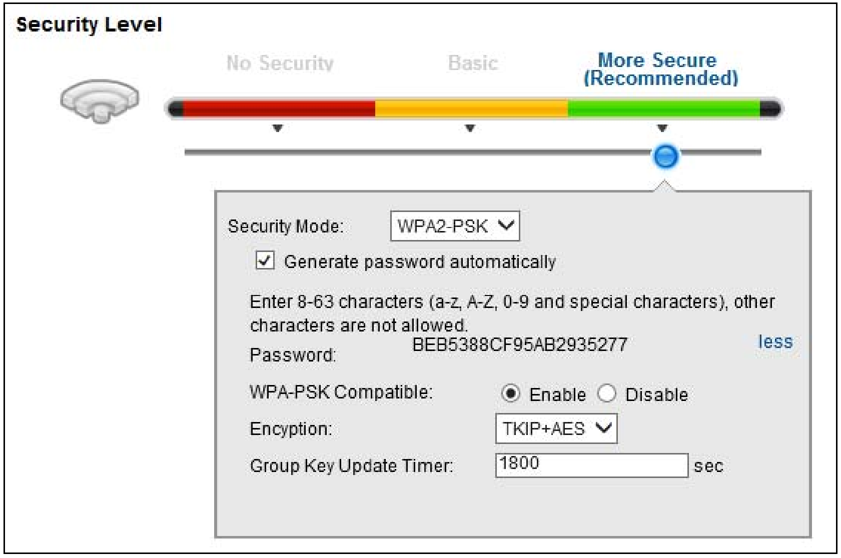
LABEL	DESCRIPTION
Security Level	Select **Basic** to enable WEP data encryption.
Generate password automatically	Select this option to have the Device automatically generate a password. The password field will not be configurable when you select this option.
Password 1~4	The password (WEP keys) are used to encrypt data. Both the Device and the wireless stations must use the same password (WEP key) for data transmission. If you chose **64-bit** WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one password, only one password can be activated at any one time. The default password is **Passowrd 1**.
more.../less	Click **more...** to show more fields in this section. Click **less** to hide them.
WEP Encryption	Select **64-bits** or **128-bits**. This dictates the length of the security key that the network is going to use.

7.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 37 Wireless > General: More Secure: WPA(2)-PSK



Security Level

Security Mode: WPA2-PSK

☑ Generate password automatically

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

Password: BEB5388CF95AB2935277

WPA-PSK Compatible: ● Enable ○ Disable

Encyption: TKIP+AES

Group Key Update Timer: 1800 sec

The following table describes the labels in this screen.

Table 22 Wireless > General: More Secure: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Generate password automatically	Select this option to have the Device automatically generate a password. The password field will not be configurable when you select this option.
Password	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
more.../less	Click **more...** to show more fields in this section. Click **less** to hide them.
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your Device. The Device supports WPA-PSK and WPA2-PSK simultaneously.

Table 22 Wireless > General: More Secure: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

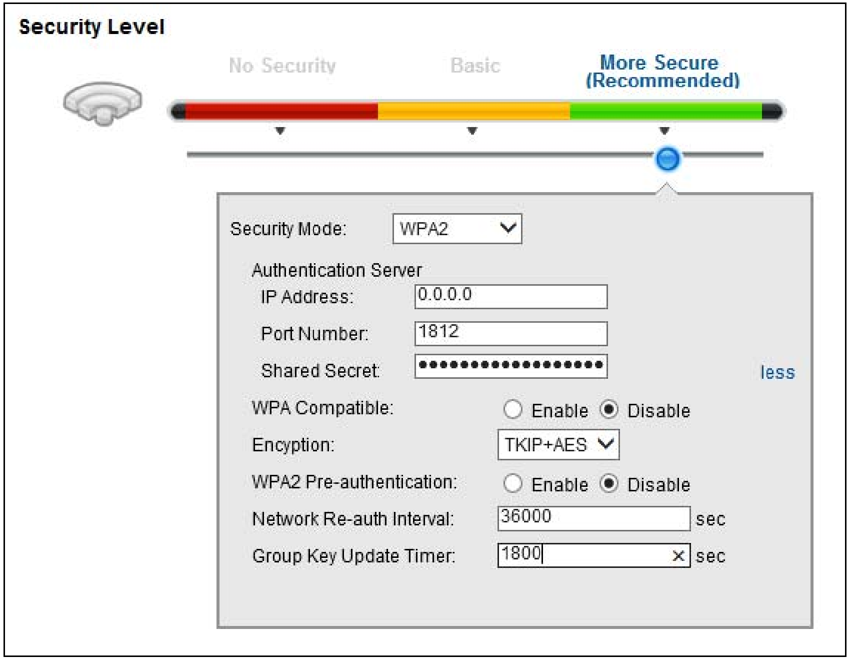
7.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA** or **WPA2** from the **Security Mode** list.

Figure 38 Wireless > General: More Secure: WPA(2)



Security Mode: WPA2

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret: •••••••••••••••••••

WPA Compatible: ○ Enable ● Disable

Encyption: TKIP+AES

WPA2 Pre-authentication: ○ Enable ● Disable

Network Re-auth Interval: 36000 sec

Group Key Update Timer: 1800 sec

The following table describes the labels in this screen.

Table 23 Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.

Table 23 Wireless > General: More Secure: WPA(2) (continued)

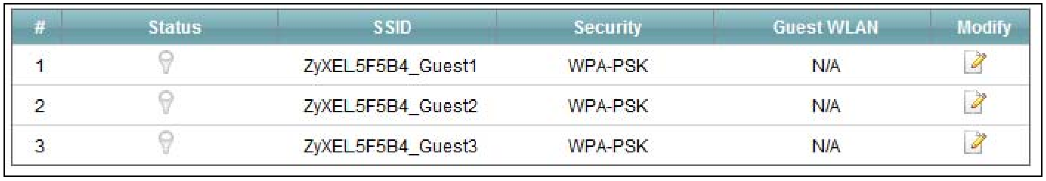
LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Device. The key must be the same on the external authentication server and your Device. The key is not sent over the network.
more.../less	Click **more...** to show more fields in this section. Click **less** to hide them.
WPA Compatible	This field is only available for WPA2. Select this if you want the Device to support WPA and WPA2 simultaneously.
Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
WPA2 Pre-Authentication	This field is available only when you select **WPA2**. Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select **Enabled** to turn on preauthentication in WAP2. Otherwise, select **Disabled**.
Network Re-auth Interval	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

7.3 The More AP Screen

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the Device.

Click **Network Setting > Wireless** > **More AP**. The following screen displays.

Figure 39 Network Setting > Wireless > More AP



#	Status	SSID	Security	Guest WLAN	Modify
1		ZyXEL5F5B4_Guest1	WPA-PSK	N/A	
2		ZyXEL5F5B4_Guest2	WPA-PSK	N/A	
3		ZyXEL5F5B4_Guest3	WPA-PSK	N/A	

The following table describes the labels in this screen.

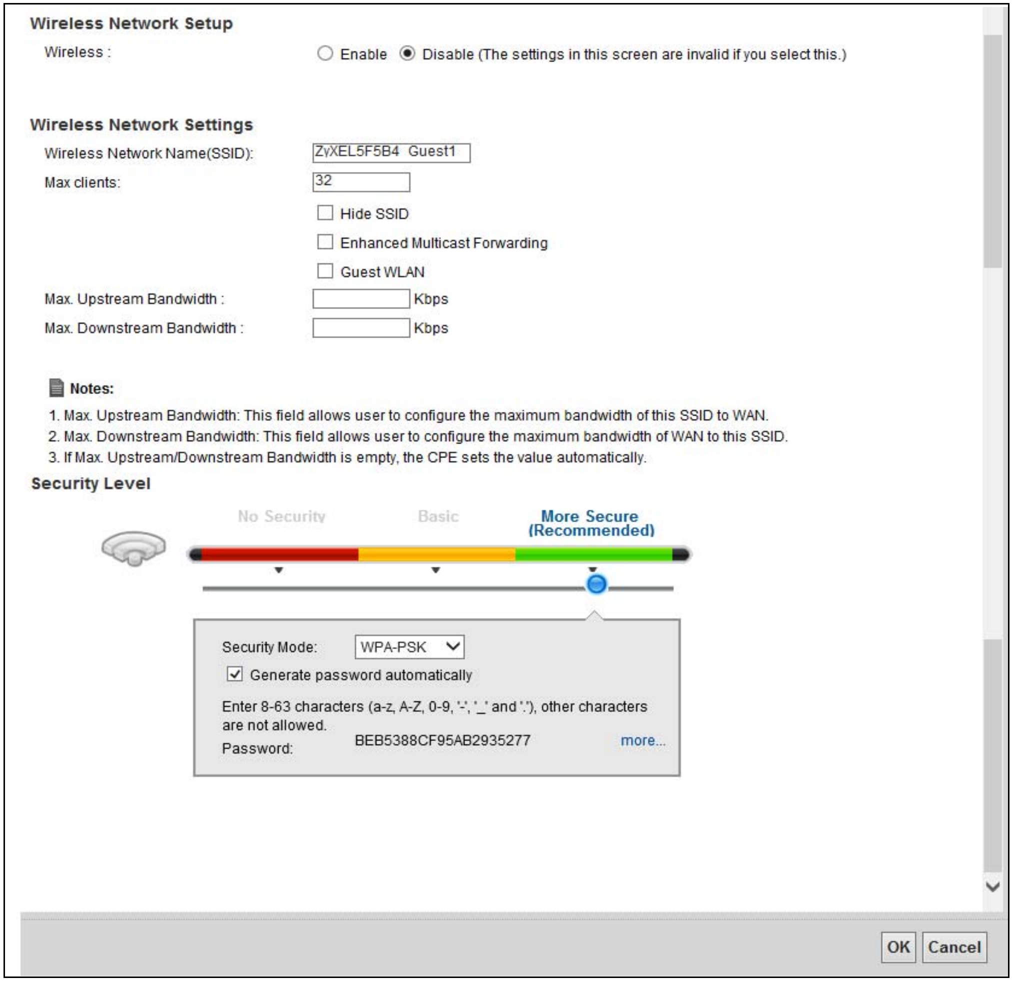
Table 24 Network Setting > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the Device’s BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.

7.3.1 Edit More AP

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 40 More AP: Edit



Wireless Network Setup

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

Wireless Network Settings

Wireless Network Name(SSID): ZyXEL5F5B4_Guest1

Max clients: 32

□ Hide SSID

□ Enhanced Multicast Forwarding

□ Guest WLAN

Max. Upstream Bandwidth : Kbps

Max. Downstream Bandwidth : Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

Security Level

Security Mode: WPA-PSK

☑ Generate password automatically

Enter 8-63 characters (a-z, A-Z, 0-9, '-', '_' and '.'), other characters are not allowed.

Password: BEB5388CF95AB2935277

The following table describes the fields in this screen.

Table 25 More AP: Edit

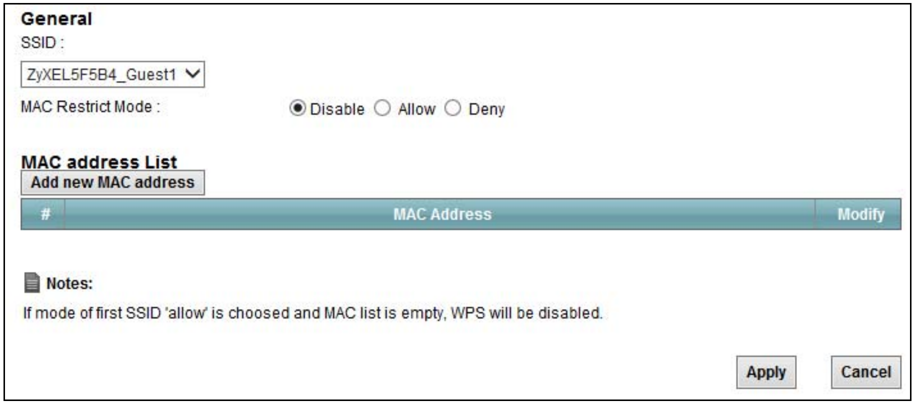
LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can **Enable** or **Disable** the wireless LAN in this field.
Passphrase Type	If you set security for the wireless LAN and have the Device generate a password, the setting in this field determines how the Device generates the password. Select **None** to set the Device's password generation to not be based on a passphrase. Select **Fixed** to use a 16 character passphrase for generating a password. Select **Variable** to use a 16 to 63 character passphrase for generating a password.
Passphrase Key	For a fixed type passphrase enter 16 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. For a variable type passphrase enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or LAN devices.
Enhanced Multicast Forwarding	Select this check box to allow the Device to convert wireless multicast traffic into wireless unicast traffic.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Maximum Bandwidth	Specify the maximum rate for wireless traffic in kilobits per second (Kbps).
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 136 for more details about this field.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

7.4 MAC Authentication

This screen allows you to configure the ZyXEL Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the ZyXEL Device **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to view your Device's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless > MAC Authentication**. The screen appears as shown.

Figure 41 Wireless > MAC Authentication



General

SSID : ZyXEL5F5B4_Guest1

MAC Restrict Mode : ● Disable ○ Allow ○ Deny

MAC address List

Notes:

If mode of first SSID 'allow' is choosed and MAC list is empty, WPS will be disabled.

The following table describes the labels in this screen.

Table 26 Wireless > MAC Authentication

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the Device. MAC addresses not listed will be allowed to access the Device. Select **Allow** to permit access to the Device. MAC addresses not listed will be denied access to the Device.
Add new MAC address	Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the wireless devices that are allowed or denied access to the Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the Device.
Modify	Click the **Delete** icon to delete the entry.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

7.5 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your Device.

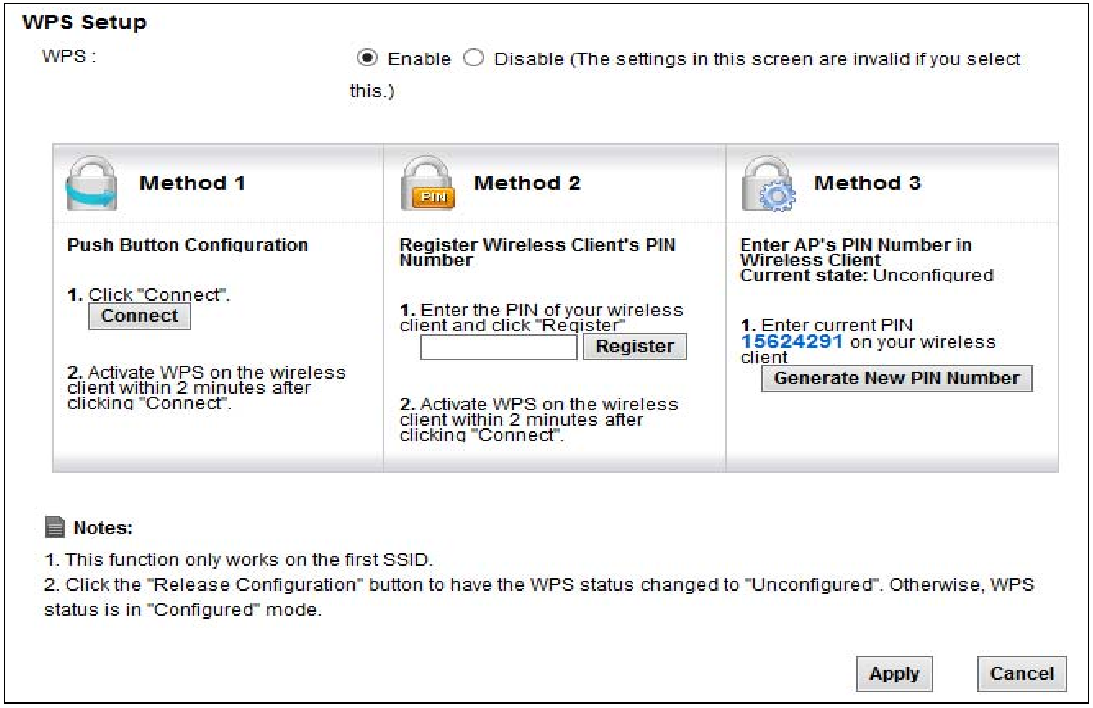
WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 7.9.8.3 on page 156 for more information about WPS.

Note: To use the WPS feature, make sure you have wireless enabled in the **Network Setting** > **Wireless** > **General** screen.

Note: The Device applies the security settings of the **SSID1** profile (see Section 7.2 on page 133). If you want to use the WPS feature set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 42 Network Setting > Wireless > WPS



WPS Setup

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

Method 1

Push Button Configuration

1. Click "Connect".
Connect

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click "Register"
Register

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

Enter AP's PIN Number in Wireless Client
Current state: Unconfigured

1. Enter current PIN 15624291 on your wireless client
Generate New PIN Number

Notes:

1. This function only works on the first SSID.
2. Click the "Release Configuration" button to have the WPS status changed to "Unconfigured". Otherwise, WPS status is in "Configured" mode.

Apply Cancel

The following table describes the labels in this screen.

Table 27 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
WPS	Select **Enable** to activate WPS on the Device.
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).

Table 27 Network Setting > Wireless > WPS (continued)

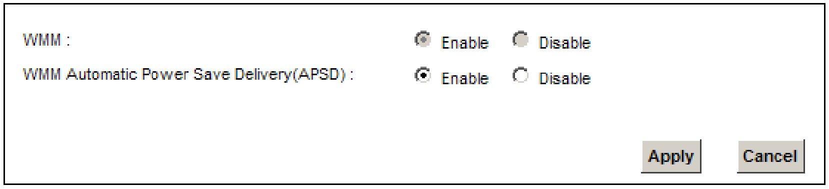
LABEL	DESCRIPTION
Connect	Click this button to add another WPS-enabled wireless device (within wireless range of the Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **Connect** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Device.
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the Device into the client.
Release Configuration	The default WPS status is configured. Click this button to remove all configured wireless and wireless security settings for WPS connections on the Device.
Generate New PIN Number	The PIN (Personal Identification Number) of the Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN Number** button to have the Device create a new PIN.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.6 The WMM Screen

Use this screen to enable Wi-Fi MultiMedia (WMM) and WMM Power Save in wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

Figure 43 Network Setting > Wireless > WMM



WMM : ● Enable ○ Disable

WMM Automatic Power Save Delivery(APSD) : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 28 Network Setting > Wireless > WMM

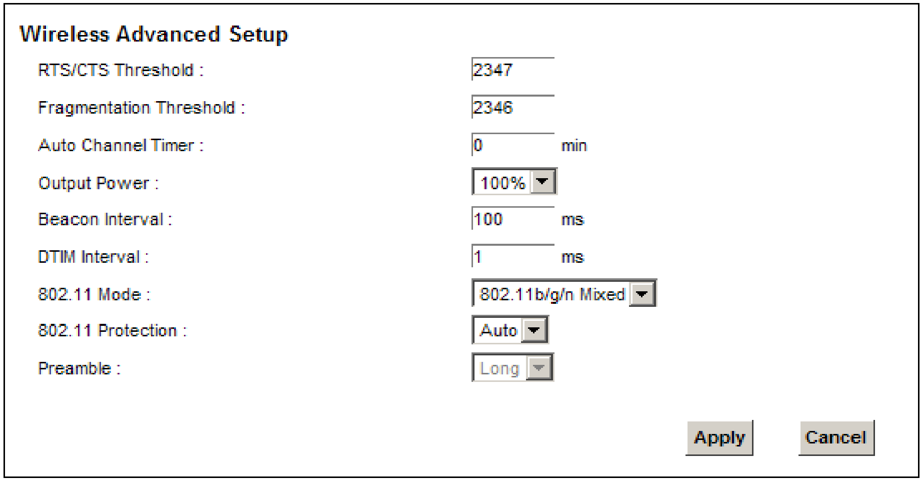
LABEL	DESCRIPTION
WMM	Select **On** to have the Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
WMM Automatic Power Save Delivery	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Device until the Device "wakes up". The Device wakes up periodically to check for incoming data. Note: Note: This works only if the wireless device to which the Device is connected also supports this feature.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.7 The Others Screen

Use this screen to configure advanced wireless settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See Section 7.9.2 on page 150 for detailed definitions of the terms listed in this screen.

Figure 44 Network Setting > Wireless > Others



Wireless Advanced Setup

RTS/CTS Threshold : 2347

Fragmentation Threshold : 2346

Auto Channel Timer : 0 min

Output Power : 100%

Beacon Interval : 100 ms

DTIM Interval : 1 ms

802.11 Mode : 802.11b/g/n Mixed

802.11 Protection : Auto

Preamble : Long

The following table describes the labels in this screen.

Table 29 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.

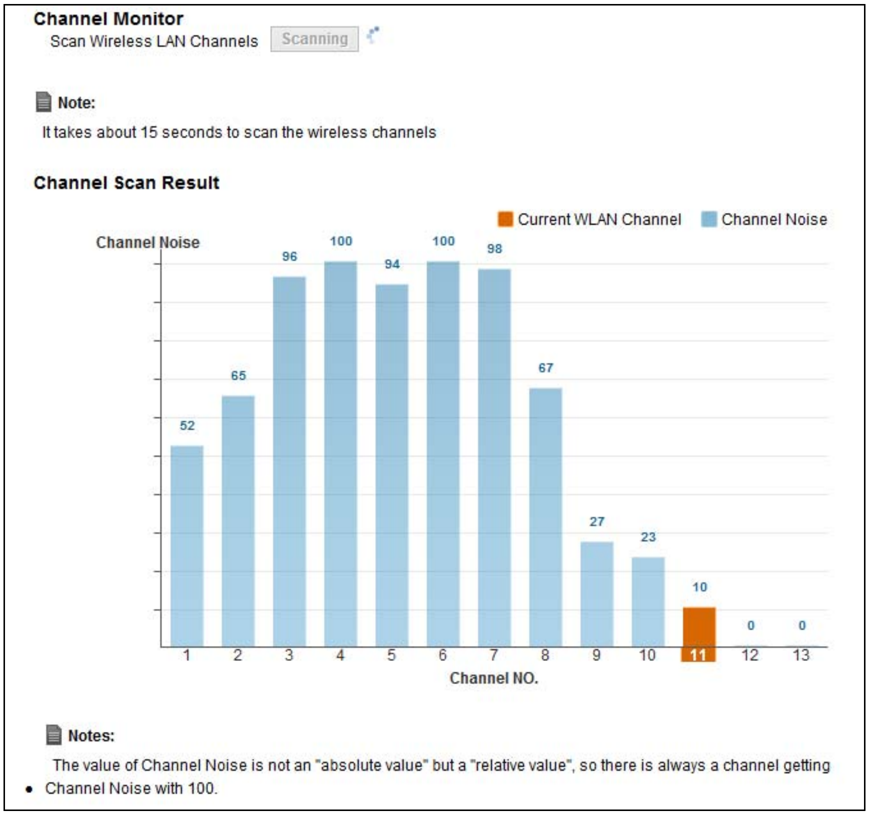
Table 29 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
Auto Channel Timer	If you set the channel to **Auto** in the **Network Setting > Wireless > General** screen, specify the interval in minutes for how often the Device scans for the best channel. Enter 0 to disable the periodical scan.
Output Power	Set the output power of the Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from20ms to 1000ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Device. Select **802.11n Only** to allow only IEEE 802.11n compliant WLAN devices to associate with the Device. Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Device. The transmission rate of the Device might be reduced when an 802.11b wireless client is associated with it. Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the Device. The transmission rate of the Device might be reduced when an 802.11b or 802.11g wireless client is associated with it.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your Device might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 7.9.7 on page 154 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.8 The Channel Status Screen

Use the **Channel Status** screen to scan wireless LAN channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **Scan** to scan the wireless LAN channels. You can view the results in the **Channel Scan Result** section.

Figure 45 Network Setting > Wireless > Channel Status



Channel Monitor

Scan Wireless LAN Channels

Note:

It takes about 15 seconds to scan the wireless channels

Channel Scan Result

Notes:

The value of Channel Noise is not an "absolute value" but a "relative value", so there is always a channel getting

- Channel Noise with 100.

7.9 Technical Reference

This section discusses wireless LANs in depth. For more information, see Appendix D on page 373.

7.9.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

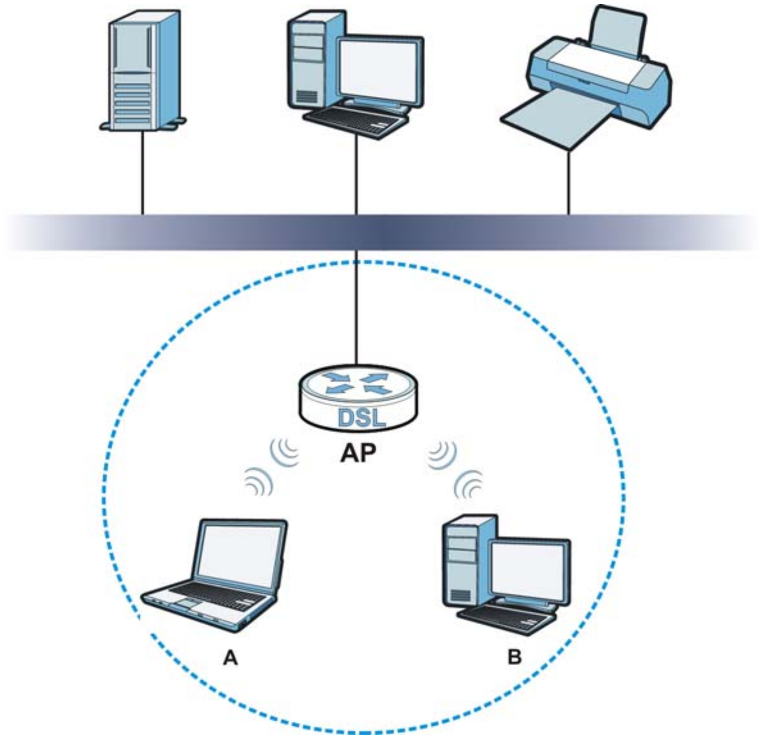
- A wireless client is a radio connected to a user’s computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network’s range.

Traditionally, a wireless network operates in one of two ways.

- An “infrastructure” type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An “ad-hoc” type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 46 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

7.9.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the Device's Web Configurator.

Table 30 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the Device does, it cannot communicate with the Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

7.9.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it’s not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use “70dodchal71vanpoi” as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

7.9.3.1 SSID

Normally, the Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

7.9.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device’s User’s Guide or other documentation.

You can use the MAC address filter to tell the Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

7.9.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

7.9.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 7.9.3.3 on page 151 for information about this.)

Table 31 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
	Static WEP	
↕	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

7.9.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

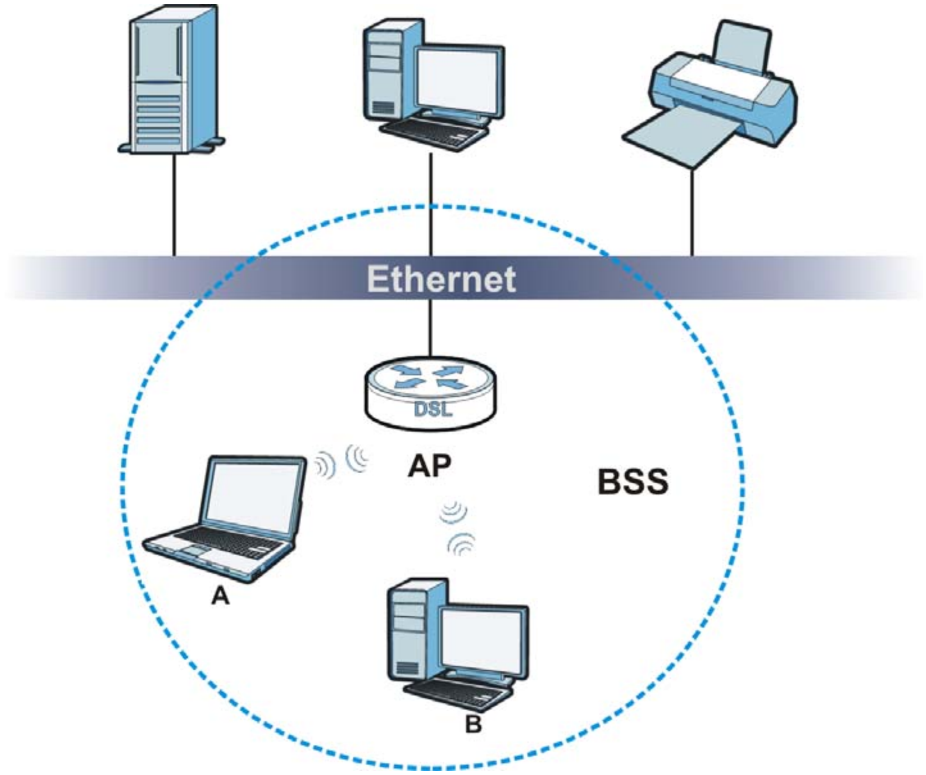
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.9.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 47 Basic Service set



7.9.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Device’s MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

7.9.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.

- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other’s communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

7.9.7 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the Device uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

7.9.8 WiFi Protected Setup (WPS)

Your Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device’s documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.9.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1 Ensure that the two devices you want to set up are within wireless range of one another.

2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Device, see Section 7.6 on page 145).

3 Press the button on one of the devices (it doesn't matter which). For the Device you must press the WPS button for more than three seconds.

4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.9.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the Device, see Section 7.5 on page 144).

4 Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within two minutes.

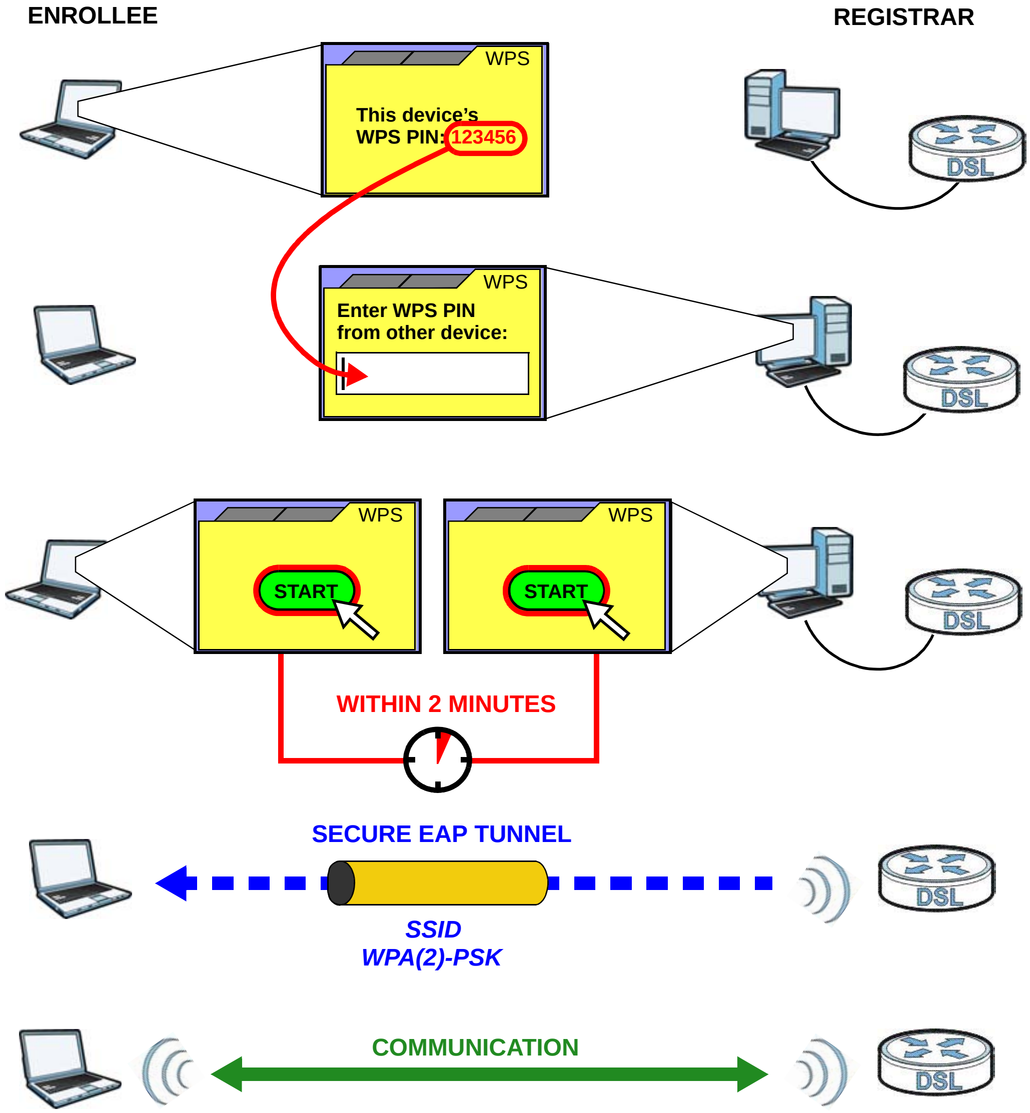
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 48 Example WPS Process: PIN Method

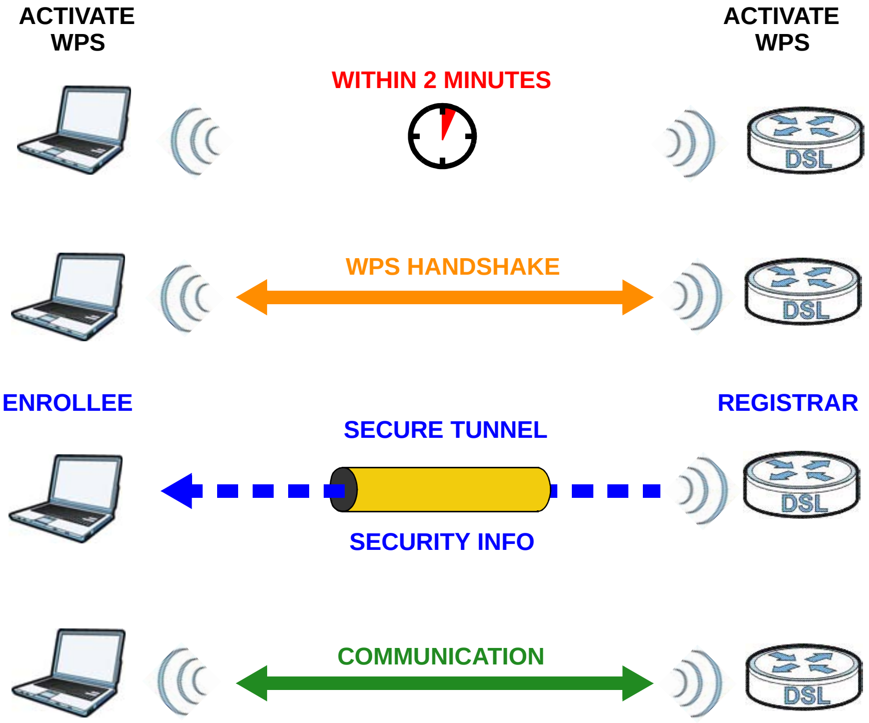


7.9.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 49 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

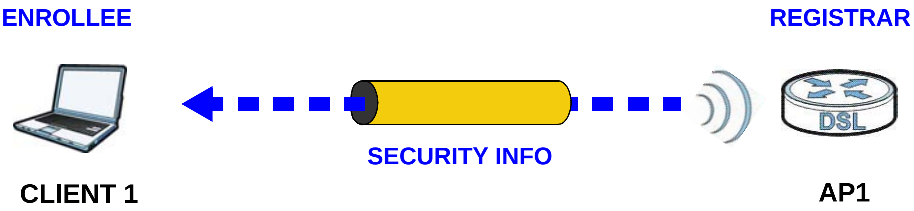
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.9.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

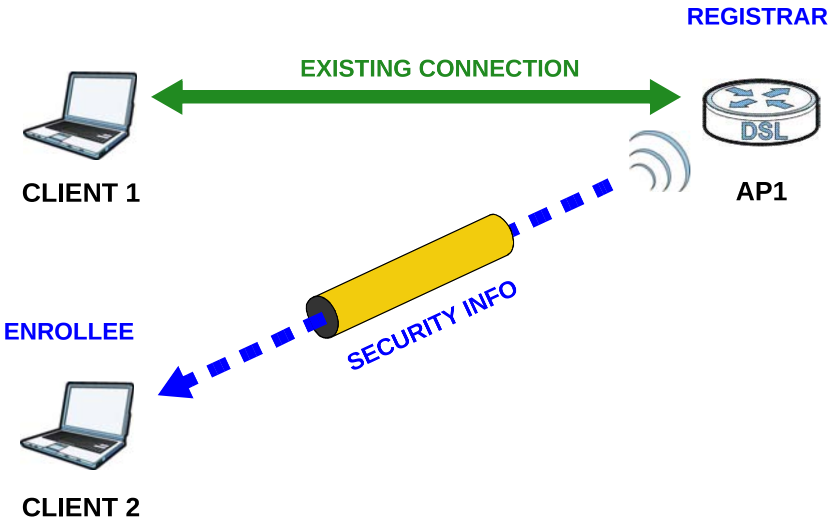
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 50 WPS: Example Network Step 1



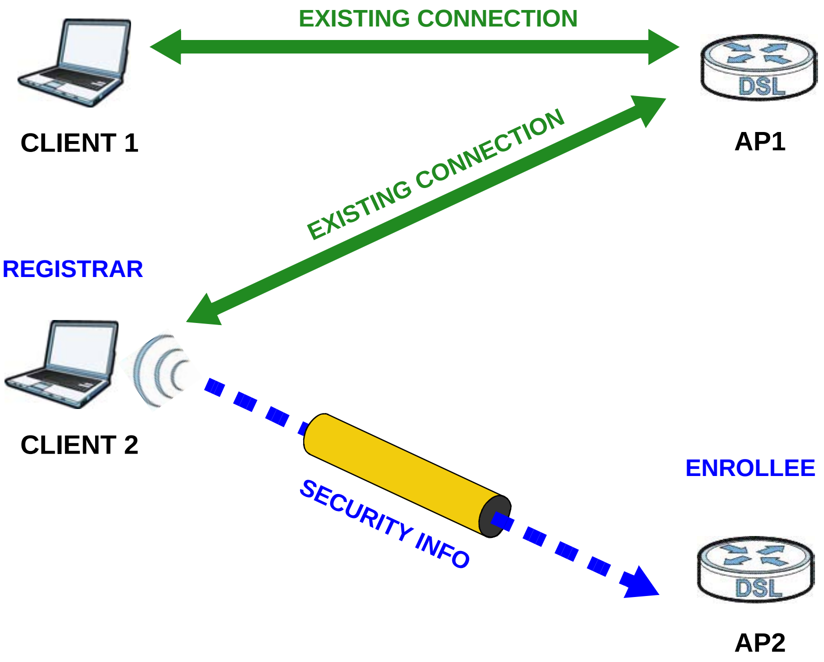
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 51 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 52 WPS: Example Network Step 3



7.9.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

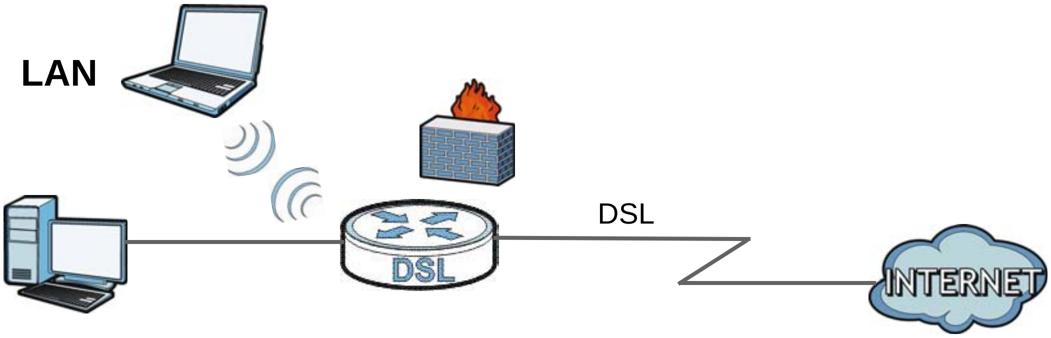
8

LAN

8.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



8.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your SBG3500-N (Section 8.2 on page 163).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 8.3 on page 167).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the SBG3500-N (Section 8.4 on page 169).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 8.5 on page 169).
- Use the **5th Ethernet Port** screen to configure the Ethernet WAN port as a LAN port (Section 8.8 on page 179).

8.1.2 What You Need To Know

8.1.2.1 About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your SBG3500-N an IP address, subnet mask, DNS and other routing information when it's turned on.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

8.1.2.2 About UPnP

Identifying UPnP Devices

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

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses

- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the Chapter 11 on page 206 for more information on NAT.

Cautions with UPnP

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

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the SBG3500-N allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

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

See Section 8.5 on page 169 for examples of installing and using UPnP.

Finding Out More

See Section 8.9 on page 179 for technical background information on LANs.

8.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

8.2 The LAN Setup Screen

Use this screen to set the Local Area Network IP address and subnet mask of your SBG3500-N. Click **Network Setting > LAN** to open the **LAN Setup** screen.

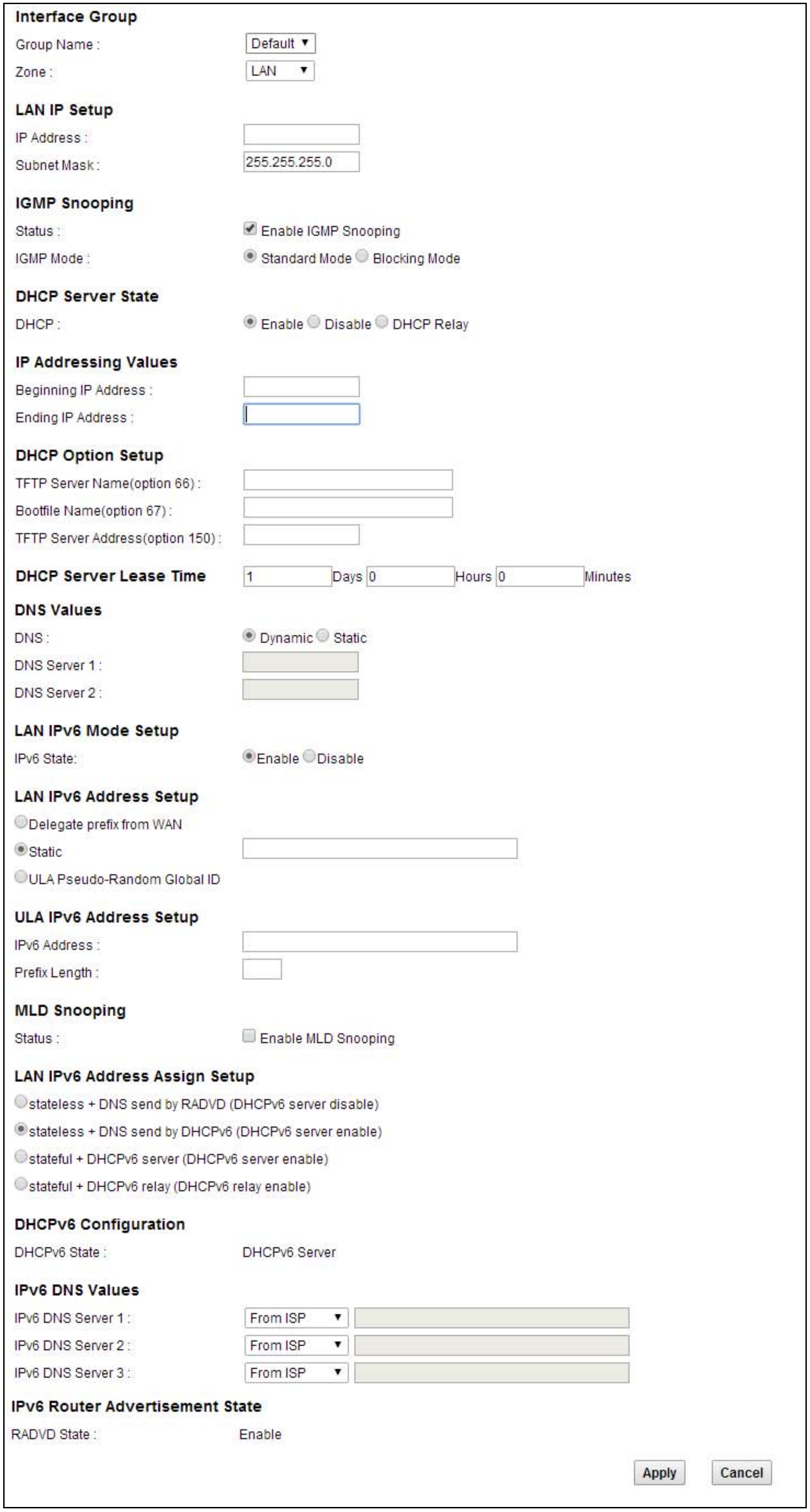
Follow these steps to configure your LAN settings.

1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your SBG3500-N.

2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

3 Click **Apply** to save your settings.

Figure 53 Network Setting > LAN > LAN Setup



Interface Group

Group Name : Default ▾

Zone : LAN ▾

LAN IP Setup

IP Address :

Subnet Mask : 255.255.255.0

IGMP Snooping

Status : ☑ Enable IGMP Snooping

IGMP Mode : ● Standard Mode ○ Blocking Mode

DHCP Server State

DHCP : ● Enable ○ Disable ○ DHCP Relay

IP Addressing Values

Beginning IP Address :

Ending IP Address :

DHCP Option Setup

TFTP Server Name(option 66) :

Bootfile Name(option 67) :

TFTP Server Address(option 150) :

DHCP Server Lease Time 1 Days 0 Hours 0 Minutes

DNS Values

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

LAN IPv6 Mode Setup

IPv6 State: ● Enable ○ Disable

LAN IPv6 Address Setup

○ Delegate prefix from WAN

● Static

○ ULA Pseudo-Random Global ID

ULA IPv6 Address Setup

IPv6 Address :

Prefix Length :

MLD Snooping

Status : □ Enable MLD Snooping

LAN IPv6 Address Assign Setup

○ stateless + DNS send by RADVD (DHCPv6 server disable)

● stateless + DNS send by DHCPv6 (DHCPv6 server enable)

○ stateful + DHCPv6 server (DHCPv6 server enable)

○ stateful + DHCPv6 relay (DHCPv6 relay enable)

DHCPv6 Configuration

DHCPv6 State : DHCPv6 Server

IPv6 DNS Values

IPv6 DNS Server 1 : From ISP ▾

IPv6 DNS Server 2 : From ISP ▾

IPv6 DNS Server 3 : From ISP ▾

IPv6 Router Advertisement State

RADVD State : Enable

The following table describes the fields in this screen.

Table 32 Network Setting > LAN > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See Chapter 13 on page 226 for how to create a new interface group.
Zone	Choose the zone for this interface group from the drop-down list.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your SBG3500-N in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your SBG3500-N automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IGMP Snooping	
Status	Select the **Enable IGMP Snooping** checkbox to allows the SBG3500-N to passively learn multicast group.
IGMP Mode	Select **Standard Mode** to have the SBG3500-N forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to have the SBG3500-N block all unknown multicast packets from the WAN.
DHCP Server State	
DHCP	Select **Enable** to have the SBG3500-N act as a DHCP server or DHCP relay agent. Select **Disable** to stop the DHCP server on the SBG3500-N. Select **DHCP Relay** to have the SBG3500-N forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select **DHCP Relay** in the **DHCP** field.
IP Address	Enter the IP address of the actual remote DHCP server in this field.
IP Addressing Values	This field is only available when you select **Enable** in the **DHCP** field.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
DHCP Option Setup	
TFTP Server Name (option 66)	Type a name for the TFTP (Trivial File Transfer Protocol) server. This field allows you to access the TFTP server using DHCP option 66. However, option 66 (open stardard) supports only the IP address of the hostname or a single TFTP server
Bootfile name (option 67)	Type the bootfile name to access the TFTP server using DHCP option 67. Option 67 is a bootstrap service that accesses the TFTP server dynamically at server startup.
TFTP Server Address (option 150)	Type an IP address for the TFTP server. This field allows you to access multiple TFTP servers using DHCP option 150. Option 150 is Cisco proprietary.

Table 32 Network Setting > LAN > LAN Setup (continued)

LABEL	DESCRIPTION
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.
Days/Hours/Minutes	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select **Enable** in the **DHCP** field.
DNS	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service.
DNS Server 1 DNS Server 2	Enter the first and second DNS (Domain Name System) server IP address the SBG3500-N passes to the DHCP clients.
LAN IPv6 Mode Setup	
IPv6 State	Select **Enable** to activate the IPv6 mode and configure IPv6 settings on the SBG3500-N.
LAN IPv6 Address Setup	
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the SBG3500-N's LAN IPv6 address. Note: This fixed address is for local hosts to access the Web Configurator only as the global LAN IPv6 address might be changed by your ISP any time. This address is not the routing gateway's address for LAN IPv6 hosts.
ULA Pseudo-Random Global ID	Select this option to get IP addresses with same prefix using the Unique Local Address Random Global ID.
ULA IPv6 Address Setup	
IPv6 Address	If you select static IPv6 address, enter the IPv6 address prefix that the SBG3500-N uses for the LAN IPv6 address.
Prefix Length	If you select static IPv6 address, enter the IPv6 prefix length that the SBG3500-N uses to generate the LAN IPv6 address. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. Select **Enable MLD Snooping** to activate MLD Snooping on the SBG3500-N. This allows the SBG3500-N to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.

Table 32 Network Setting > LAN > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: • **stateless + DNS send by RADVD:** The SBG3500-N uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the SBG3500-N send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. (See page 162 for more information on RADVD.) • **stateless + DNS send by DHCPv6**: The SBG3500-N uses IPv6 stateless autoconfiguration. The DNS is provided by a DHCPv6 server. • **stateful + DHCPv6 server:** The SBG3500-N uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the SBG3500-N act as a DHCPv6 server and pass IPv6 addresses, DNS server and domain name information to DHCPv6 clients. • **stateful + DHCPv6 relay:** The SBG3500-N uses IPv6 stateful autoconfiguration. **DHCPv6 Relay** is enabled to have the SBG3500-N relay client DHCPv6 requests.
DHCPv6 Configuration	
DHCPv6 State	This shows the status of the DHCPv6.
IPv6 DNS Values	
IPv6 DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns IPv6 DNS server information. Select **User-Defined** if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the SBG3500-N passes to the DHCP clients. Select **None** if you do not want to configure IPv6 DNS servers.
IPv6 Router Advertisement State	
RADVD State	This shows the status of RADVD.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

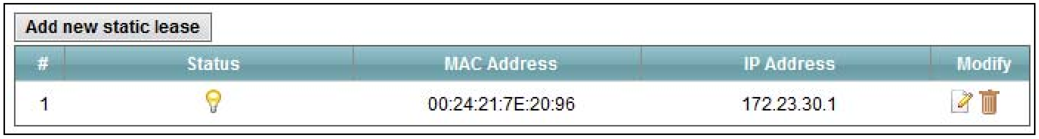
8.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Use this screen to change your SBG3500-N's static DHCP settings. Click **Network Setting > LAN > Static DHCP** to open the following screen.

Figure 54 Network Setting > LAN > Static DHCP



#	Status	MAC Address	IP Address	Modify
1	💡	00:24:21:7E:20:96	172.23.30.1	✎ 🗑

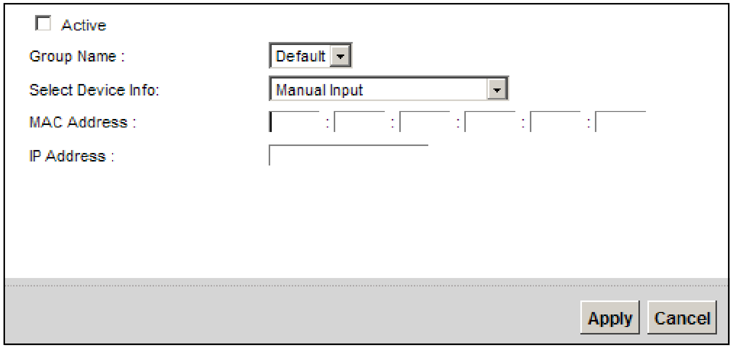
The following table describes the labels in this screen.

Table 33 Network Setting > LAN > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the SBG3500-N.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the **Edit** icon to have the IP address field editable and change it. Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

If you click **Add new static lease** in the **Static DHCP** screen or the Edit icon next to a static DHCP entry, the following screen displays.

Figure 55 Static DHCP: Add/Edit



□ Active

Group Name : Default

Select Device Info: Manual Input

MAC Address : __ : __ : __ : __ : __ : __

IP Address :

The following table describes the labels in this screen.

Table 34 Static DHCP: Add/Edit

LABEL	DESCRIPTION
Active	Select this to activate the connection between the client and the SBG3500-N.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Chapter 13 on page 226 for how to create a new interface group.
Select Device Info	If you select **Manual Input**, you can manually type in the MAC address and IP address of a computer on your LAN. You can also choose the name of a computer from the drop list and have the MAC Address and IP Address auto-detected.
MAC Address	If you select **Manual Input**, enter the MAC address of a computer on your LAN.
IP Address	If you select **Manual Input**, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

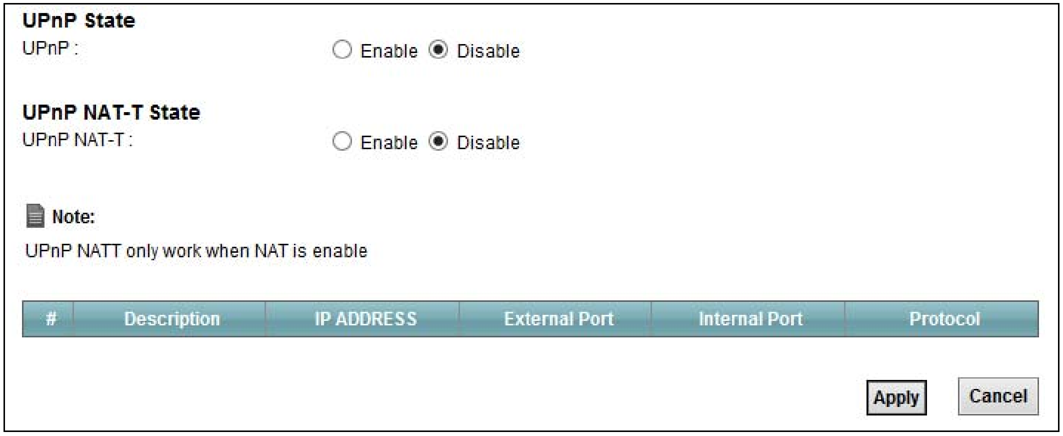
8.4 The UPnP Screen

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

See page 162 for more information on UPnP.

Use the following screen to configure the UPnP settings on your SBG3500-N. Click **Network Setting > LAN > UPnP** to display the screen shown next.

Figure 56 Network Setting > LAN > UPnP



UPnP State

UPnP : ○ Enable ● Disable

UPnP NAT-T State

UPnP NAT-T : ○ Enable ● Disable

Note:

UPnP NATT only work when NAT is enable

#	Description	IP ADDRESS	External Port	Internal Port	Protocol

The following table describes the labels in this screen.

Table 35 Network Setting > LAN > UPnP

LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the SBG3500-N's IP address (although you must still enter the password to access the web configurator).
UPnP NAT-T	Select **Enable** to allow UPnP-enabled applications to automatically configure the SBG3500-N so that they can communicate through the SBG3500-N by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

8.5 Installing UPnP in Windows Example

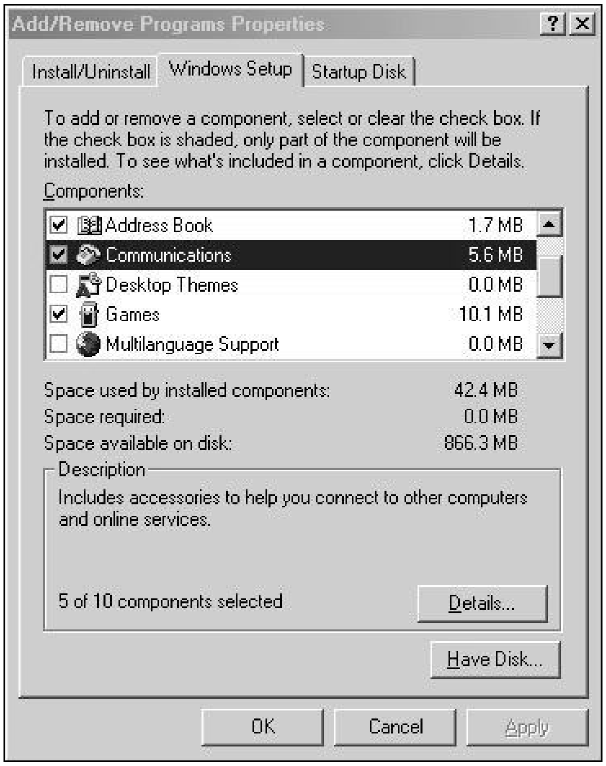
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



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

Components:

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

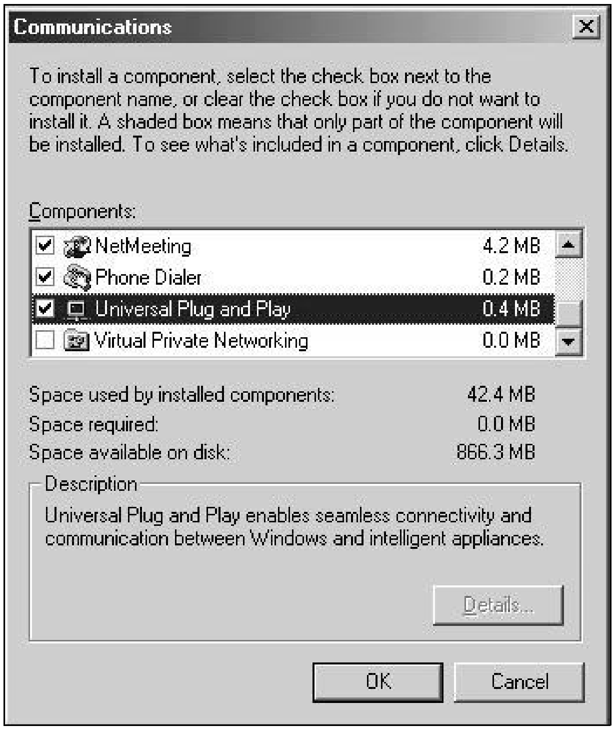
Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

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

5 of 10 components selected

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



Communications

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

Components:

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

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

Description

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

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

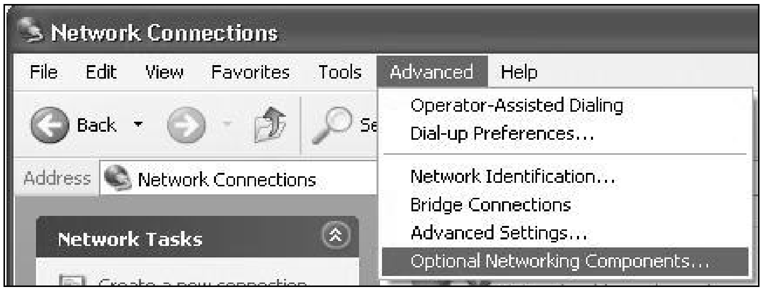
Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

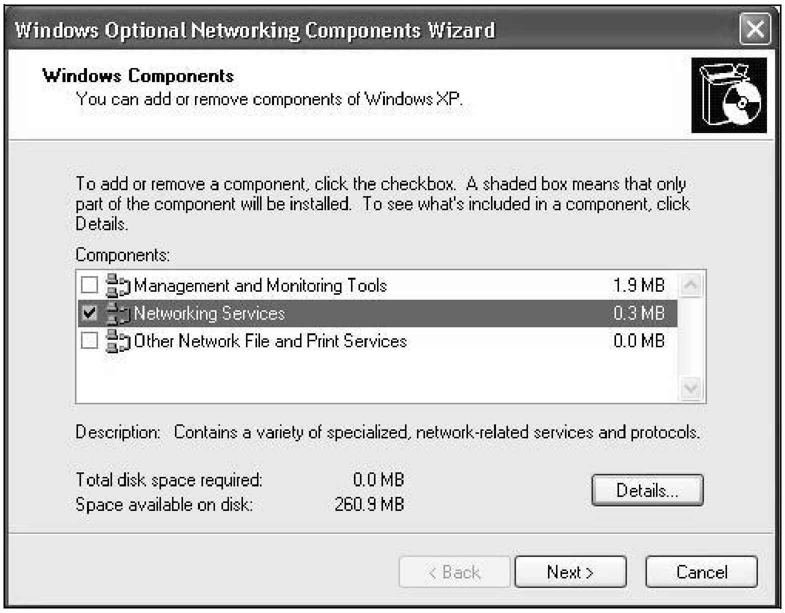
1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.



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



Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows XP.

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

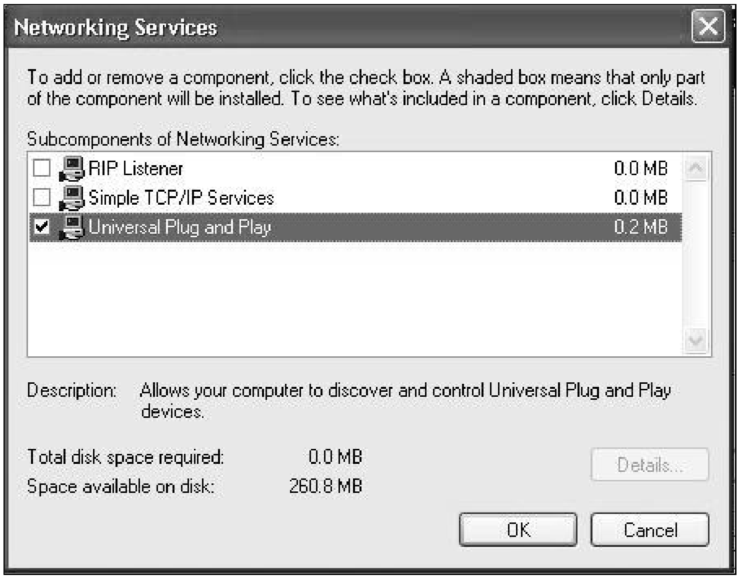
Components:

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

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

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

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



Networking Services

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

Subcomponents of Networking Services:

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

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

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

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

8.6 Using UPnP in Windows XP Example

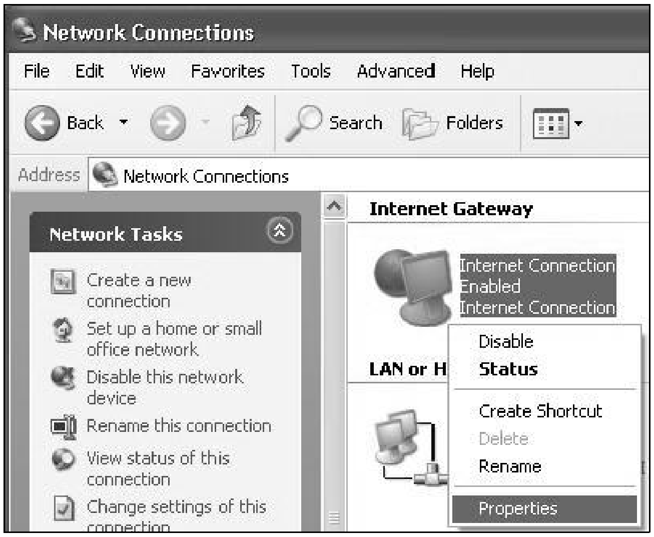
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the SBG3500-N.

Make sure the computer is connected to a LAN port of the SBG3500-N. Turn on your computer and the SBG3500-N.

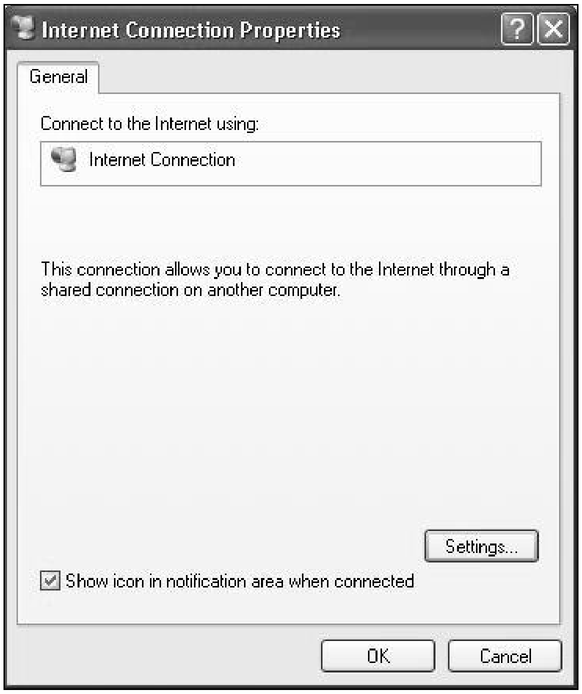
Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.



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


Internet Connection Properties
General

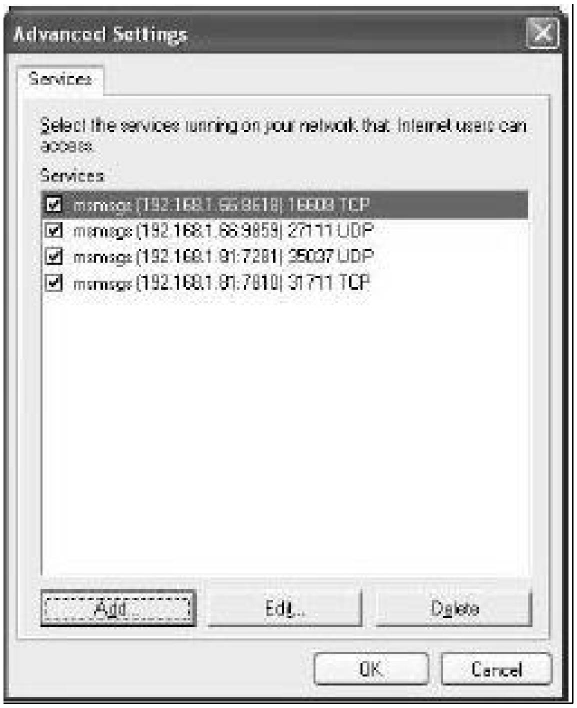
Connect to the Internet using:

Internet Connection

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

Settings...
☑ Show icon in notification area when connected
OK
Cancel

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



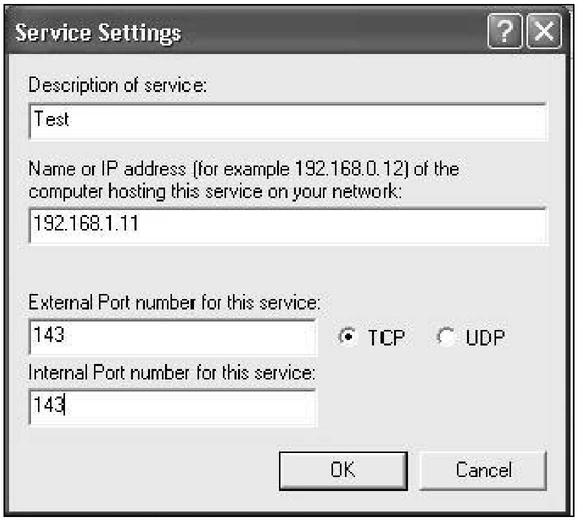
Advanced Settings

Services

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

Services

- ☑ msmsgs (192.168.1.66:8618) 16608 TCP
- ☑ msmsgs (192.168.1.66:9859) 27111 UDP
- ☑ msmsgs (192.168.1.91:7281) 35037 UDP
- ☑ msmsgs (192.168.1.91:7810) 31711 TCP



Service Settings

Description of service: Test

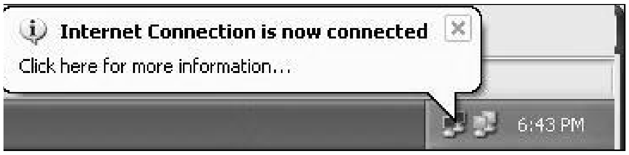
Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network: 192.168.1.11

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

Internal Port number for this service: 143

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

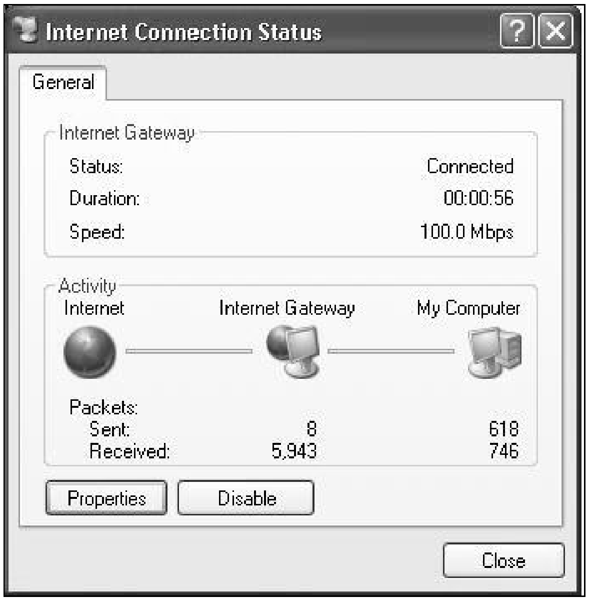
6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.



Internet Connection is now connected

Click here for more information...

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



Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

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

Web Configurator Easy Access

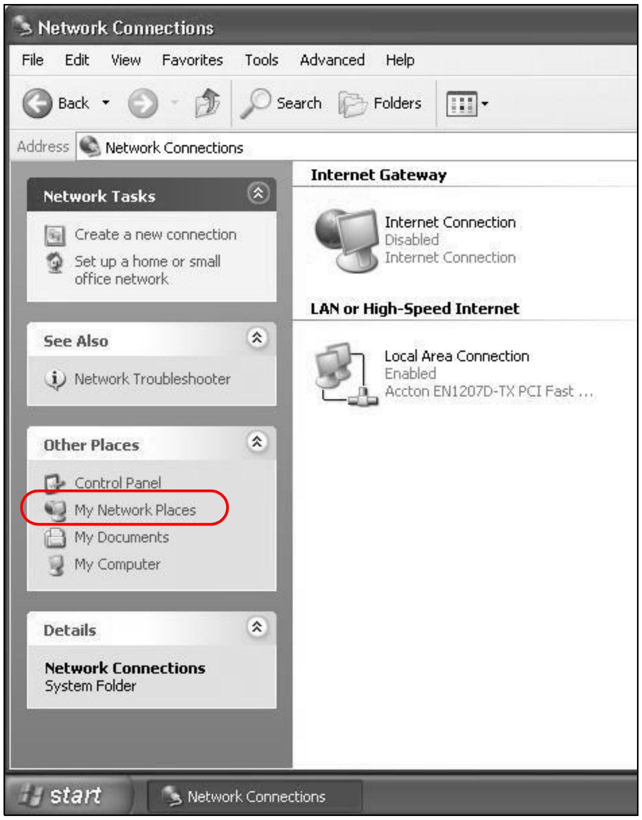
With UPnP, you can access the web-based configurator on the SBG3500-N without finding out the IP address of the SBG3500-N first. This comes helpful if you do not know the IP address of the SBG3500-N.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

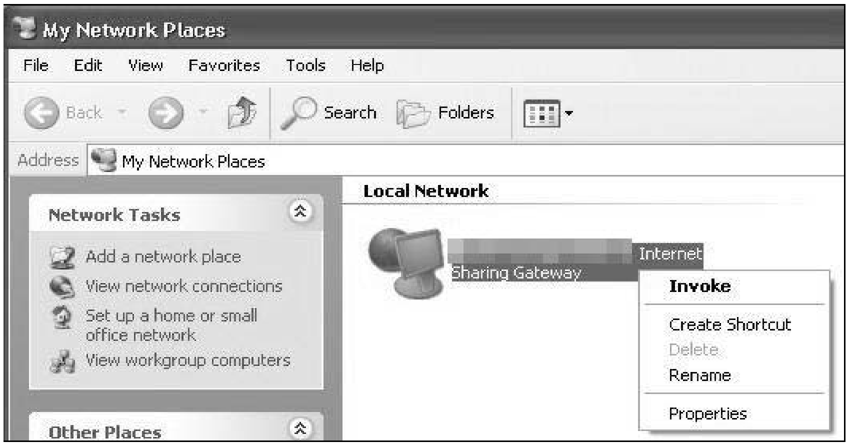
2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

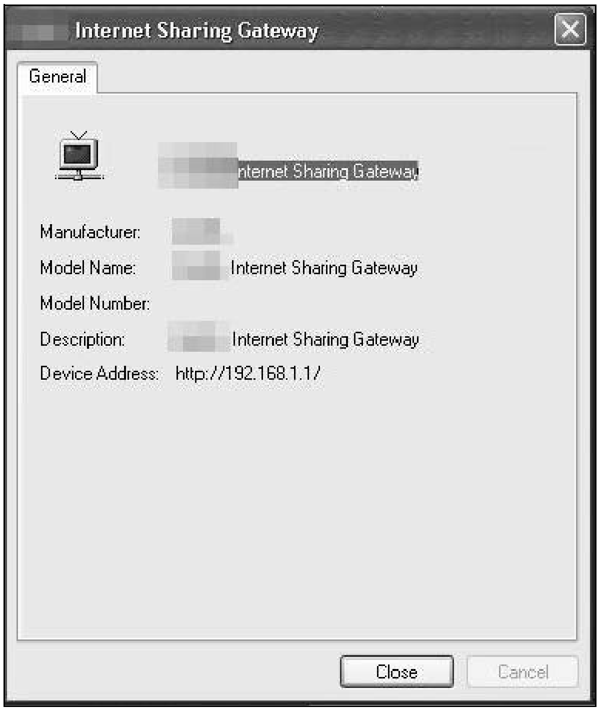


4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your SBG3500-N and select **Invoke**. The web configurator login screen displays.



6 Right-click on the icon for your SBG3500-N and select **Properties**. A properties window displays with basic information about the SBG3500-N.



[redacted] Internet Sharing Gateway

Manufacturer: [redacted]

Model Name: [redacted] Internet Sharing Gateway

Model Number:

Description: [redacted] Internet Sharing Gateway

Device Address: http://192.168.1.1/

8.7 The Additional Subnet Screen

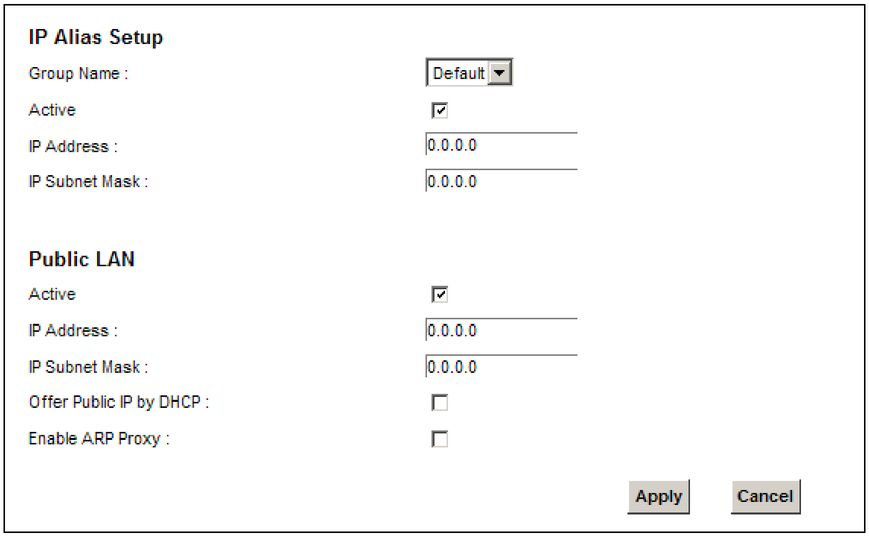
Use the **Additional Subnet** screen to configure IP alias and public static IP.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The SBG3500-N supports multiple logical LAN interfaces via its physical Ethernet interface with the SBG3500-N itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

If your ISP provides the Public LAN service, the SBG3500-N may use an LAN IP address that can be accessed from the WAN.

Click **Network Setting > LAN > Additional Subnet** to display the screen shown next.

Figure 57 Network Setting > LAN > Additional Subnet



IP Alias Setup

Group Name :	Default
Active	☑
IP Address :	0.0.0.0
IP Subnet Mask :	0.0.0.0

Public LAN

Active	☑
IP Address :	0.0.0.0
IP Subnet Mask :	0.0.0.0
Offer Public IP by DHCP :	□
Enable ARP Proxy :	□

The following table describes the labels in this screen.

Table 36 Network Setting > LAN > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Chapter 13 on page 226 for how to create a new interface group.
Active	Select the checkbox to configure a LAN network for the SBG3500-N.
IP Address	Enter the IP address of your SBG3500-N in dotted decimal notation.
IP Subnet Mask	Your SBG3500-N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the SBG3500-N.
Public LAN	
Active	Select the checkbox to enable the Public LAN feature. Your ISP must support Public LAN and Static IP.
IP Address	Enter the public IP address provided by your ISP.
IP Subnet Mask	Enter the public IP subnet mask provided by your ISP.

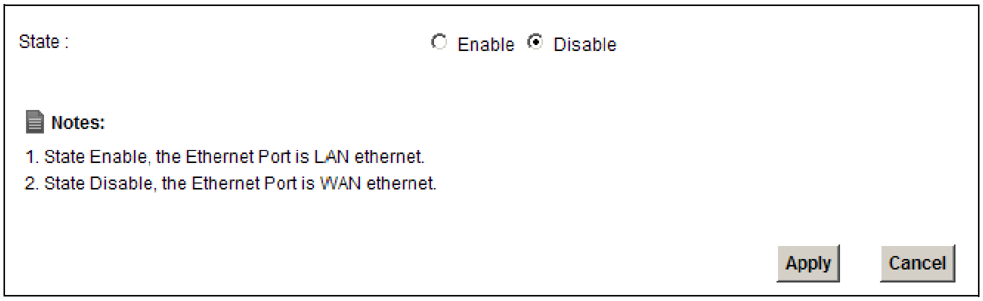
Table 36 Network Setting > LAN > Additional Subnet (continued)

LABEL	DESCRIPTION
Offer Public IP by DHCP	Select the checkbox to enable the SBG3500-N to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select the checkbox to enable the ARP (Address Resolution Protocol) proxy.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

8.8 The 5th Ethernet Port Screen

If you are using DSL connection, you can configure your Ethernet WAN port as an extra LAN port. This fifth Ethernet port is a Gigabit port. Click **Network Settings > LAN > 5th Ethernet Port** to open this screen.

Figure 58 Network Settings > LAN > 5th Ethernet Port



State : ○ Enable ● Disable

Notes:

1. State Enable, the Ethernet Port is LAN ethernet.
2. State Disable, the Ethernet Port is WAN ethernet.

The following table describes the fields in this screen.

Table 37 Network Settings > LAN > 5th Ethernet Port

LABEL	DESCRIPTION
State	Select **Enable** to use the Ethernet WAN port as a LAN port on the SBG3500-N.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to exit this screen without saving.

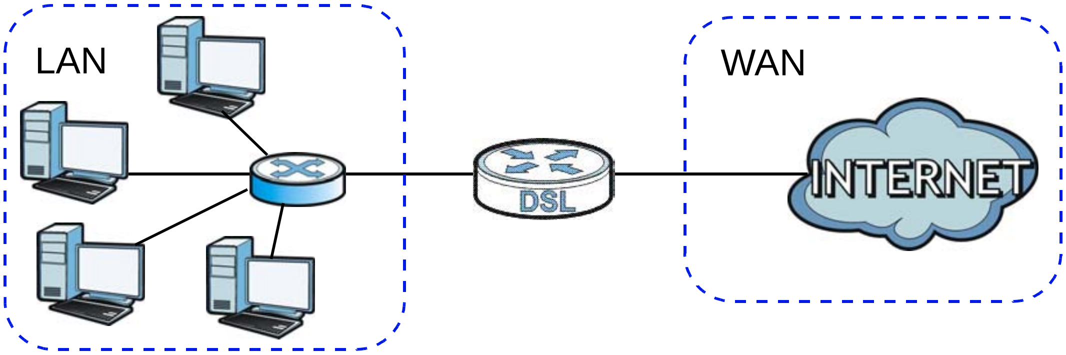
8.9 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

8.9.1 LANs, WANs and the SBG3500-N

The actual physical connection determines whether the SBG3500-N ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 59 LAN and WAN IP Addresses



8.9.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the SBG3500-N as a DHCP server or disable it. When configured as a server, the SBG3500-N provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The SBG3500-N is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

8.9.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.

- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The SBG3500-N supports the IPCP DNS server extensions through the DNS proxy feature.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

8.9.4 LAN TCP/IP

The SBG3500-N has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the SBG3500-N. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your SBG3500-N, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your SBG3500-N will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the SBG3500-N unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

9

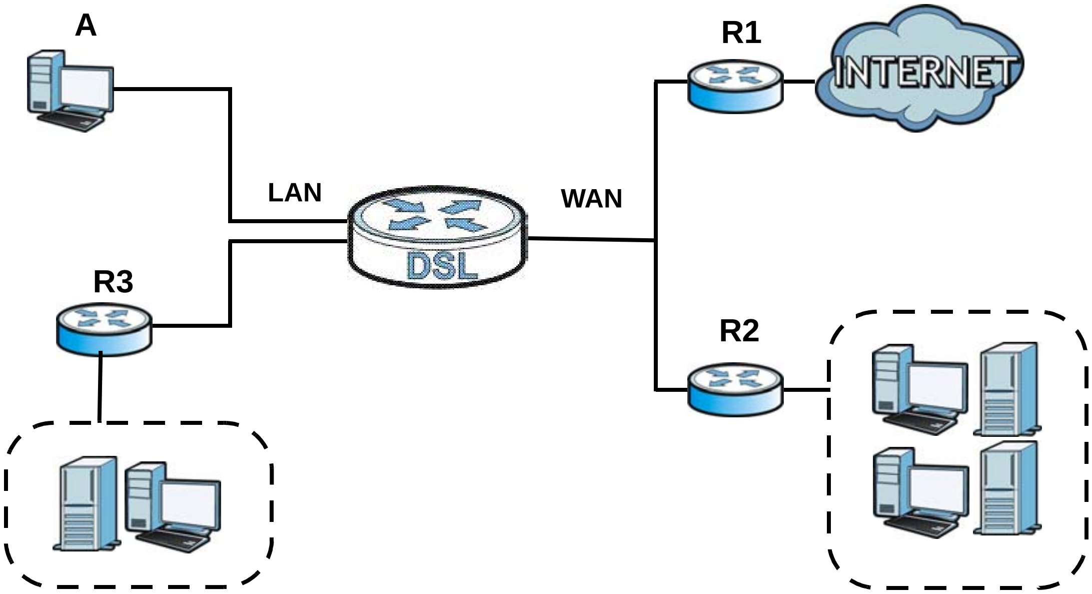
Routing

9.1 Overview

The Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Device’s LAN interface. The Device routes most traffic from **A** to the Internet through the Device’s default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 60 Example of Routing Topology



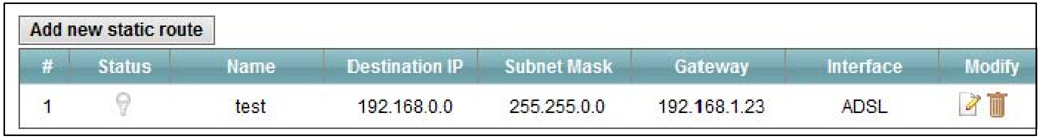
9.1.1 What You Can Do in this Chapter

- Use the **Static Route** screen to view and set up static routes on the Device (Section 9.2 on page 184).
- Use the **Policy Forwarding** screen to configure policy routing on the Device. (Section 9.3 on page 185).
- Use the **RIP** screen to set up RIP settings on the Device. (Section 9.4 on page 187).

9.2 The Routing Screen

Use this screen to view and configure the static route rules on the Device. Click **Network Setting > Routing > Static Route** to open the following screen.

Figure 61 Network Setting > Routing > Static Route



Add new static route

#	Status	Name	Destination IP	Subnet Mask	Gateway	Interface	Modify
1		test	192.168.0.0	255.255.0.0	192.168.1.23	ADSL	

The following table describes the labels in this screen.

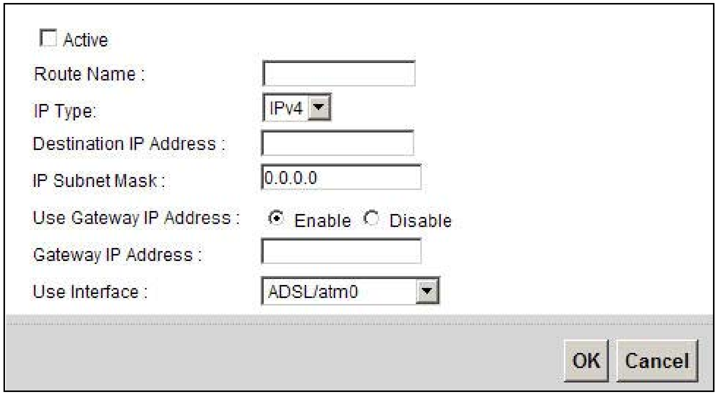
Table 38 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add new static route	Click this to configure a new static route.
#	This is the index number of the entry.
Status	This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface used for this static route.
Modify	Click the **Edit** icon to edit the static route on the Device. Click the **Delete** icon to remove a static route from the Device. A window displays asking you to confirm that you want to delete the route.

9.2.1 Add/Edit Static Route

Use this screen to add or edit a static route. Click **Add new static route** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

Figure 62 Routing: Add/Edit



☐ Active

Route Name :

IP Type: IPv4

Destination IP Address :

IP Subnet Mask : 0.0.0.0

Use Gateway IP Address : ● Enable ○ Disable

Gateway IP Address :

Use Interface : ADSL/atm0

The following table describes the labels in this screen.

Table 39 Routing: Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route. Select this to enable the static route. Clear this to disable this static route without having to delete the entry.
Route Name	Enter a descriptive name for the static route.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
IP Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. If you want to use the gateway IP address, select **Enable**.
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

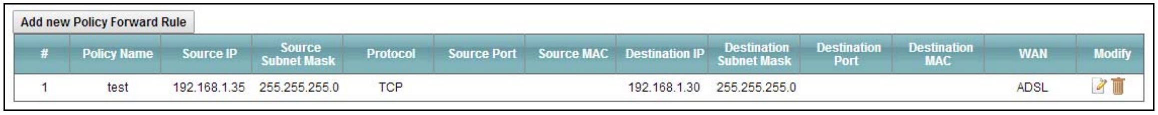
9.3 The Policy Forwarding Screen

Traditionally, routing is based on the destination address only and the Device takes the shortest path to forward a packet. Policy forwarding allows the Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

The **Policy Forwarding** screen let you view and configure routing policies on the Device. Click **Network Setting > Routing > Policy Forwarding** to open the following screen.

Figure 63 Network Setting > Routing > Policy Forwarding



#	Policy Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Destination IP	Destination Subnet Mask	Destination Port	Destination MAC	WAN	Modify
1	test	192.168.1.35	255.255.255.0	TCP			192.168.1.30	255.255.255.0			ADSL	

The following table describes the labels in this screen.

Table 40 Network Setting > Routing >Policy Forwarding

LABEL	DESCRIPTION
Add new Policy Forward Rule	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.

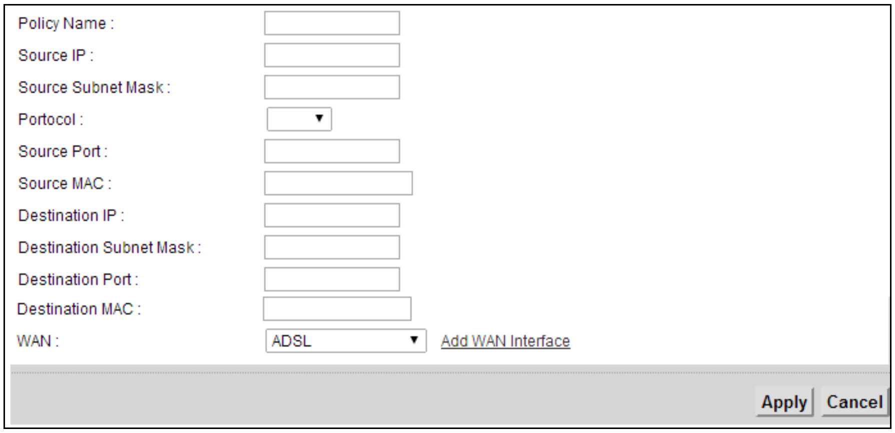
Table 40 Network Setting > Routing >Policy Forwarding (continued)

LABEL	DESCRIPTION
Policy Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Source MAC	This is the source MAC address
Destination IP	This is the destination IP address.
Destination Subnet Mask	This is the destination subnet mask address.
Destination Port	This is the destination port number.
Destination MAC	This is the destination MAC address.
WAN	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to edit this policy. Click the **Delete** icon to remove a policy from the Device. A window displays asking you to confirm that you want to delete the policy.

9.3.1 Add/Edit Policy Forwarding

Click **Add new Policy Forward Rule** in the **Policy Forwarding** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 64 Policy Forwarding: Add/Edit



Policy Name :

Source IP :

Source Subnet Mask :

Portocol :

Source Port :

Source MAC :

Destination IP :

Destination Subnet Mask :

Destination Port :

Destination MAC :

WAN : ADSL

The following table describes the labels in this screen.

Table 41 Policy Forwarding: Add/Edit (Sheet 1 of 2)

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP	Enter the source IP address.

Table 41 Policy Forwarding: Add/Edit (Sheet 2 of 2)

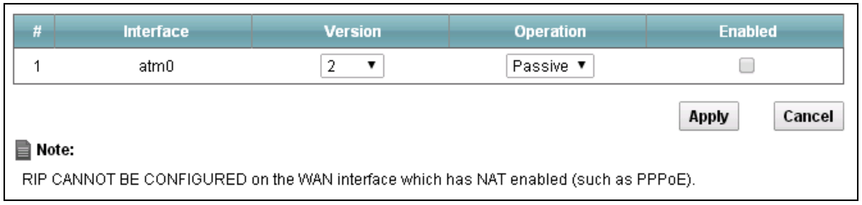
LABEL	DESCRIPTION
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Destination IP	Enter the destination IP address.
Destination Subnet Mask	Enter the destination subnet mask address.
Destination Port	Enter the destination port.
Destination MAC	Enter the destination MAC address.
WAN	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screens.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

9.4 The RIP Screen

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

Click **Network Setting > Routing > RIP** to open the **RIP** screen.

Figure 65 RIP



#	Interface	Version	Operation	Enabled
1	atm0	2 ▼	Passive ▼	□

Note:

RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

The following table describes the labels in this screen.

Table 42 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Device sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select **Passive** to have the Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the Device advertise its route information and also listen for routing updates from neighboring routers.

Table 42 Network Setting > Routing > RIP

LABEL	DESCRIPTION
Enabled	Select the check box to activate the settings.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10

Quality of Service (QoS)

10.1 Overview

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

Configure QoS on the Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1. Configure classifiers to sort traffic into different flows.

2. Assign priority and define actions to be performed for a classified traffic flow.

The Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

10.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 10.3 on page 191).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 10.4 on page 192).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 10.5 on page 194).
- The **Policer Setup** screen lets you add, edit or delete QoS policers (Section 10.5 on page 194).
- The **Monitor** screen lets you view the Device's QoS-related packet statistics (Section 10.7 on page 201).

10.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

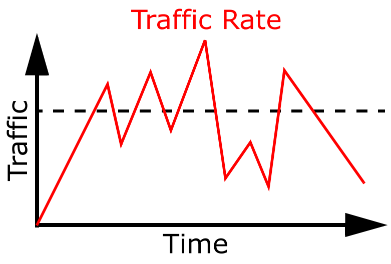
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

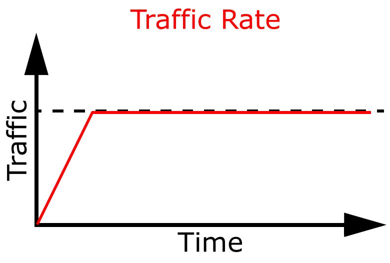
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



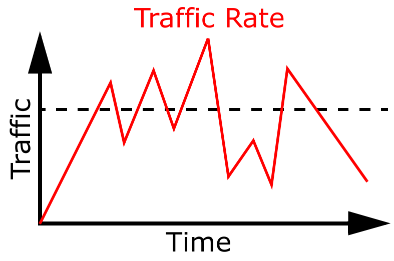
(Before Traffic Shaping)



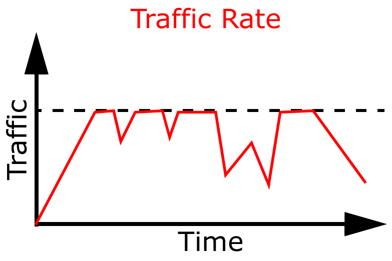
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

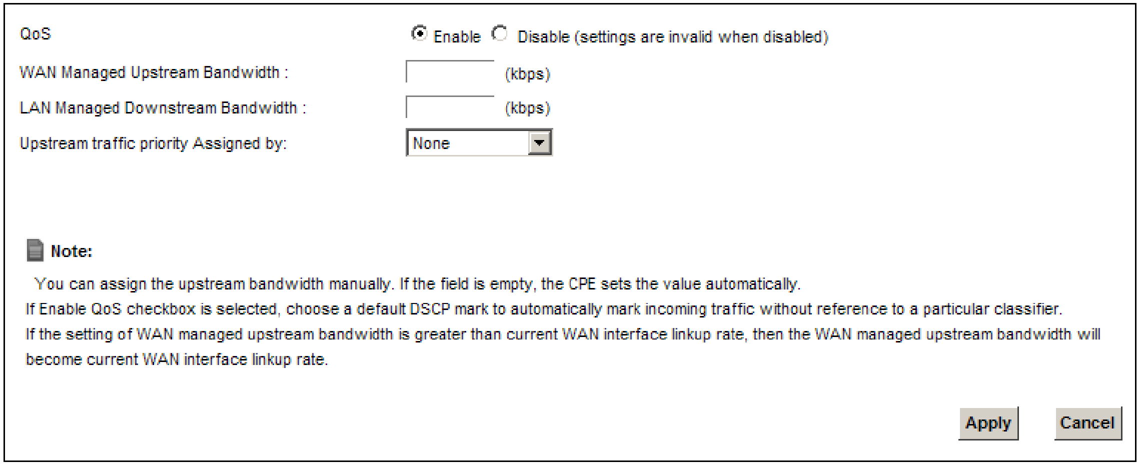
The Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 10.8 on page 202 for more information on each metering algorithm.

10.3 The Quality of Service General Screen

Click **Network Setting > QoS > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth. See Section 10.1 on page 189 for more information.

Figure 66 Network Settings > QoS > General



QoS	● Enable ○ Disable (settings are invalid when disabled)
WAN Managed Upstream Bandwidth :	(kbps)
LAN Managed Downstream Bandwidth :	(kbps)
Upstream traffic priority Assigned by:	None

Note:

You can assign the upstream bandwidth manually. If the field is empty, the CPE sets the value automatically.
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

The following table describes the labels in this screen.

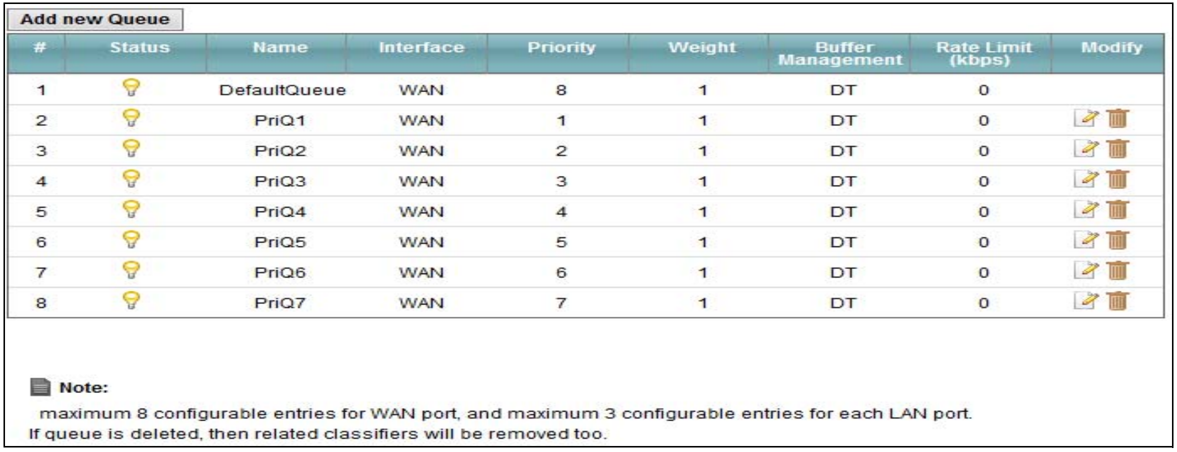
Table 43 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Select the **Enable** check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interfaces' actual transmission speed. The Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed. You can also set this number lower than the interfaces' actual transmission speed. This will cause the Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.
LAN Managed Downstream Bandwidth	Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS. The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection. You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the Device automatically sets this to the LAN interfaces' maximum supported connection speed.
Upstream traffic priority Assigned by	Select how the Device assigns priorities to various upstream traffic flows. • **None:** Disables auto priority mapping and has the Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • **Ethernet Priority:** Automatically assign priority based on the IEEE 802.1p priority level. • **IP Precedence:** Automatically assign priority based on the first three bits of the TOS field in the IP header. • **Packet Length:** Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort • data packets like file transfers.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.4 The Queue Setup Screen

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment.



Add new Queue

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
1	💡	DefaultQueue	WAN	8	1	DT	0	
2	💡	PriQ1	WAN	1	1	DT	0	✎ 🗑
3	💡	PriQ2	WAN	2	1	DT	0	✎ 🗑
4	💡	PriQ3	WAN	3	1	DT	0	✎ 🗑
5	💡	PriQ4	WAN	4	1	DT	0	✎ 🗑
6	💡	PriQ5	WAN	5	1	DT	0	✎ 🗑
7	💡	PriQ6	WAN	6	1	DT	0	✎ 🗑
8	💡	PriQ7	WAN	7	1	DT	0	✎ 🗑

Note:
maximum 8 configurable entries for WAN port, and maximum 3 configurable entries for each LAN port.
If queue is deleted, then related classifiers will be removed too.

Figure 67 Network Setting > QoS > Queue Setup

The following table describes the labels in this screen.

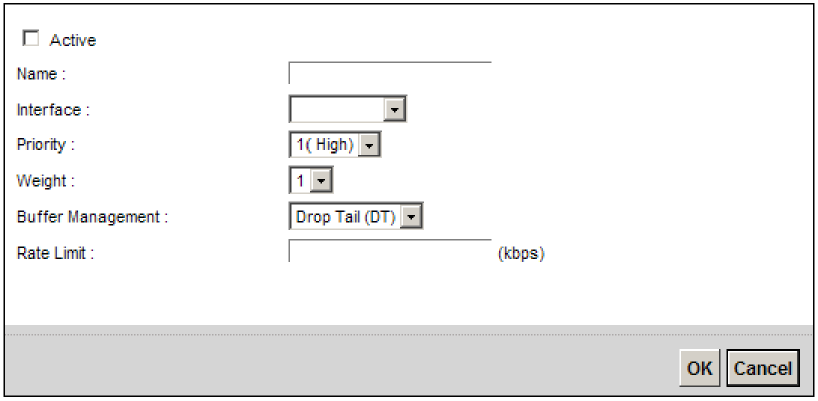
Table 44 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Device should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

10.4.1 Adding a QoS Queue

Click **Add new Queue** or the edit icon in the **Queue Setup** screen to configure a queue.

Figure 68 Queue Setup: Add



☐ Active

Name :

Interface :

Priority : 1(High)

Weight : 1

Buffer Management : Drop Tail (DT)

Rate Limit : (kbps)

The following table describes the labels in this screen.

Table 45 Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue. Note that \"<>%\\^[]`\+\$\,='#&@.:() are not allowed.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

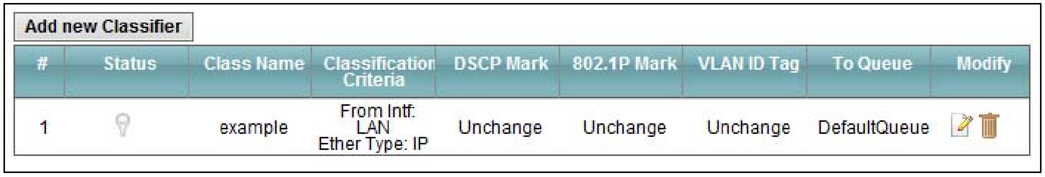
10.5 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

Figure 69 Network Setting > QoS > Class Setup



#	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
1		example	From Intf: LAN Ether Type: IP	Unchange	Unchange	Unchange	DefaultQueue	

The following table describes the labels in this screen.

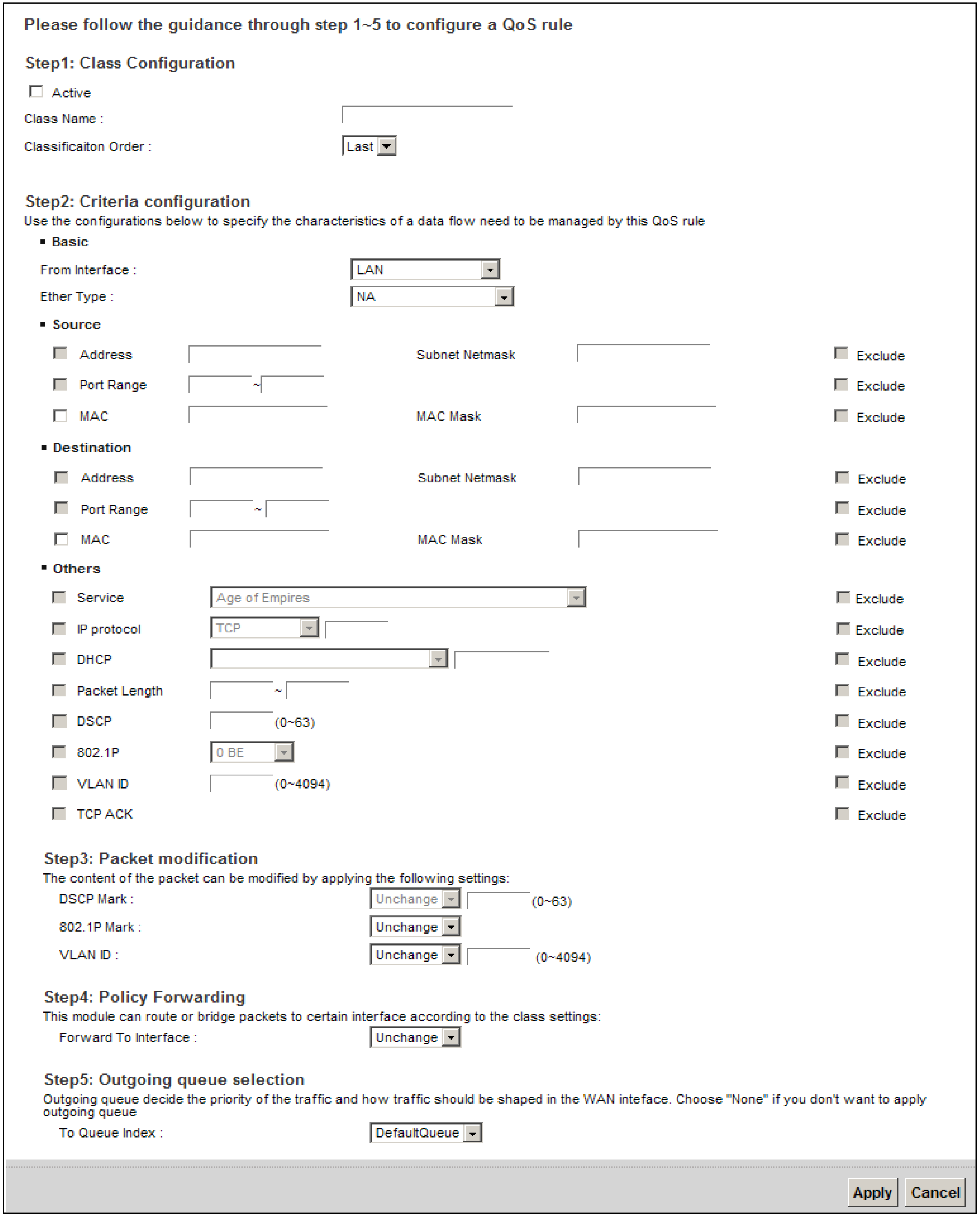
Table 46 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
#	This is the index number of the entry.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

10.5.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 70 Class Setup: Add/Edit



Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

□ Active

Class Name :

Classificaiton Order : Last

Step2: Criteria configuration

Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

- **Basic**

From Interface : LAN

Ether Type : NA

- **Source**

□ Address — Subnet Netmask — □ Exclude

□ Port Range ~ — □ Exclude

□ MAC — MAC Mask — □ Exclude

- **Destination**

□ Address — Subnet Netmask — □ Exclude

□ Port Range ~ — □ Exclude

□ MAC — MAC Mask — □ Exclude

- **Others**

□ Service — Age of Empires — □ Exclude

□ IP protocol — TCP — □ Exclude

□ DHCP — □ Exclude

□ Packet Length ~ — □ Exclude

□ DSCP (0~63) — □ Exclude

□ 802.1P — 0 BE — □ Exclude

□ VLAN ID (0~4094) — □ Exclude

□ TCP ACK — □ Exclude

Step3: Packet modification

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

DSCP Mark : Unchange (0~63)

802.1P Mark : Unchange

VLAN ID : Unchange (0~4094)

Step4: Policy Forwarding

This module can route or bridge packets to certain interface according to the class settings:

Forward To Interface : Unchange

Step5: Outgoing queue selection

Outgoing queue decide the priority of the traffic and how traffic should be shaped in the WAN inteface. Choose "None" if you don't want to apply outgoing queue

To Queue Index : DefaultQueue

The following table describes the labels in this screen.

Table 47 Class Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select this to enable this classifier.
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the **From Interface** drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **802.1Q**, you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 47 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Service	This field is available only when you select **IP** in the **Ether Type** field. This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP**, **UDP**, **ICMP** or **IGMP**. If you select **User defined**, enter the protocol (service type) number.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user’s category or application type in the matched DHCP packets.
Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
DSCP Mark	This field is available only when you select **IP** in the **Ether Type** field. If you select **Mark**, enter a DSCP value with which the Device replaces the DSCP field in the packets. If you select **Unchange**, the Device keep the DSCP field in the packets.
802.1P Mark	Select a priority level with which the Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the Device keep the 802.1p priority field in the packets.
VLAN ID	If you select **Remark**, enter a VLAN ID number with which the Device replaces the VLAN ID of the frames. If you select **Remove**, the Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the Device keep the VLAN ID in the packets.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the Device forward traffic of this class according to the default routing table.

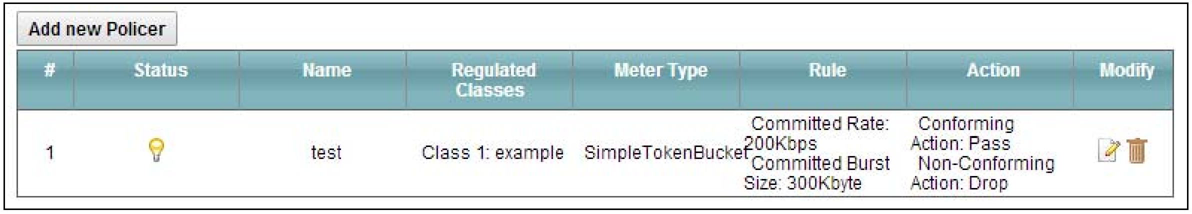
Table 47 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.6 The QoS Policer Setup Screen

Use this screen to configure QoS policers that allow you to limit the transmission rate of incoming traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

Figure 71 Network Setting > QoS > Policer Setup



#	Status	Name	Regulated Classes	Meter Type	Rule	Action	Modify
1	💡	test	Class 1: example	SimpleTokenBucket	Committed Rate: 200Kbps Committed Burst Size: 300Kbyte	Conforming Action: Pass Non-Conforming Action: Drop	✎ 🗑

The following table describes the labels in this screen.

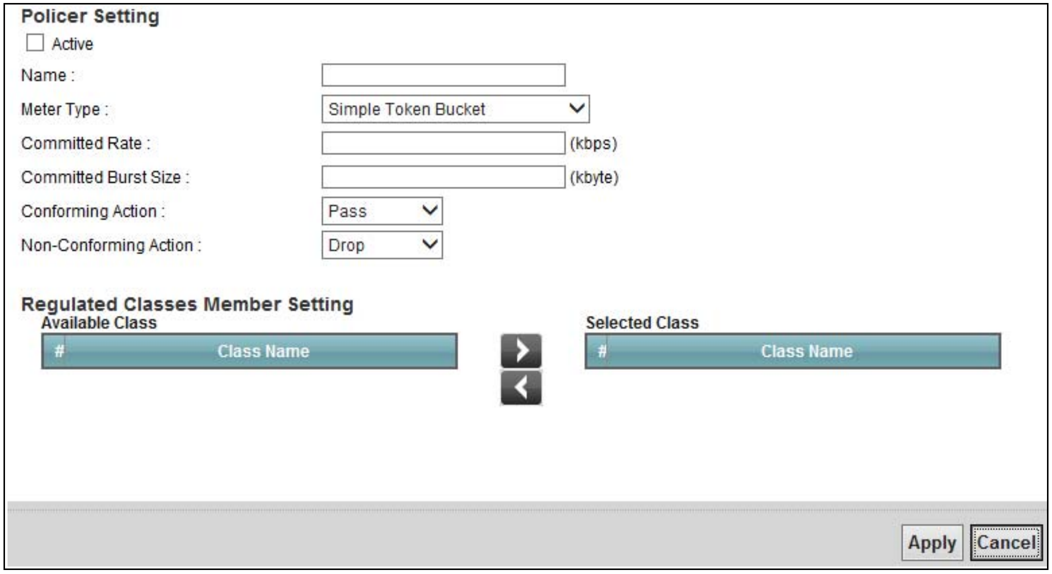
Table 48 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add new Policer	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier.
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows the how the policer has the Device treat different types of traffic belonging to the policer’s member QoS classes.
Modify	Click the **Edit** icon to edit the policer. Click the **Delete** icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

10.6.1 Add/Edit a QoS Policer

Click **Add new Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 72 Policer Setup: Add/Edit



Policer Setting

□ Active

Name :

Meter Type : Simple Token Bucket

Committed Rate : (kbps)

Committed Burst Size : (kbyte)

Conforming Action : Pass

Non-Conforming Action : Drop

Regulated Classes Member Setting

Available Class

#	Class Name

Selected Class

#	Class Name

The following table describes the labels in this screen.

Table 49 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to activate this policer.
Name	Enter the descriptive name of this policer.
Meter Type	This shows the traffic metering algorithm used in this policer. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size. The **Single Rate Three Color Marker** (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The **Two Rate Three Color Marker** (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Conforming Action	Specify what the Device does for packets within the committed rate and burst size (green-marked packets). • **Pass:** Send the packets without modification. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use.

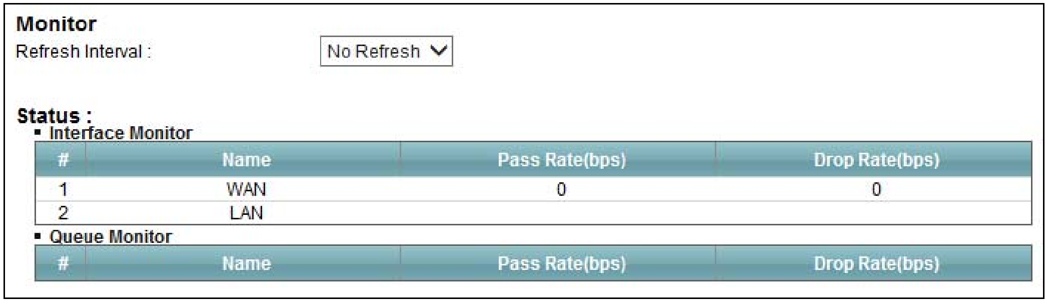
Table 49 Policer Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Non-Conforming Action	Specify what the Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). • **Drop:** Discard the packets. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Available Class Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.7 The QoS Monitor Screen

To view the Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

Figure 73 Network Setting > QoS > Monitor



Monitor

Refresh Interval : No Refresh

Status :

▪ Interface Monitor

#	Name	Pass Rate(bps)	Drop Rate(bps)
1	WAN	0	0
2	LAN		

▪ Queue Monitor

#	Name	Pass Rate(bps)	Drop Rate(bps)

The following table describes the labels in this screen.

Table 50 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the Device to update this screen. Select **No Refresh** to stop refreshing statistics.
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the interface on the Device.
Pass Rate	This shows how many packets forwarded to this interface are transmitted successfully.
Drop Rate	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate	This shows how many packets assigned to this queue are dropped.

10.8 Technical Reference

The following section contains additional technical information about the Device features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 51 IEEE 802.1p Priority Level and Traffic Type

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

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the Device, the Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the Device. On the Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 52 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250

Table 52 Internal Layer2 and Layer3 QoS Mapping

	LAYER 2	LAYER 3		
PRIORITY QUEUE	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Device treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface’s capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

11

Network Address Translation (NAT)

11.1 Overview

This chapter discusses how to configure NAT on the Device. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 11.2 on page 207).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network (Section 11.3 on page 210).
- Use the **Port Triggering** screen to add and configure the Device's trigger port settings (Section 11.4 on page 211).
- Use the **Default Server** screen to configure a default server (Section 11.5 on page 214).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the Device (Section 11.6 on page 215).
- Use the **Address Mapping** screen to configure the Device's address mapping settings (Section 11.7 on page 215).

11.1.2 What You Need To Know

Inside/Outside

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the

WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section 11.8 on page 217 for advanced technical information on NAT.

11.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

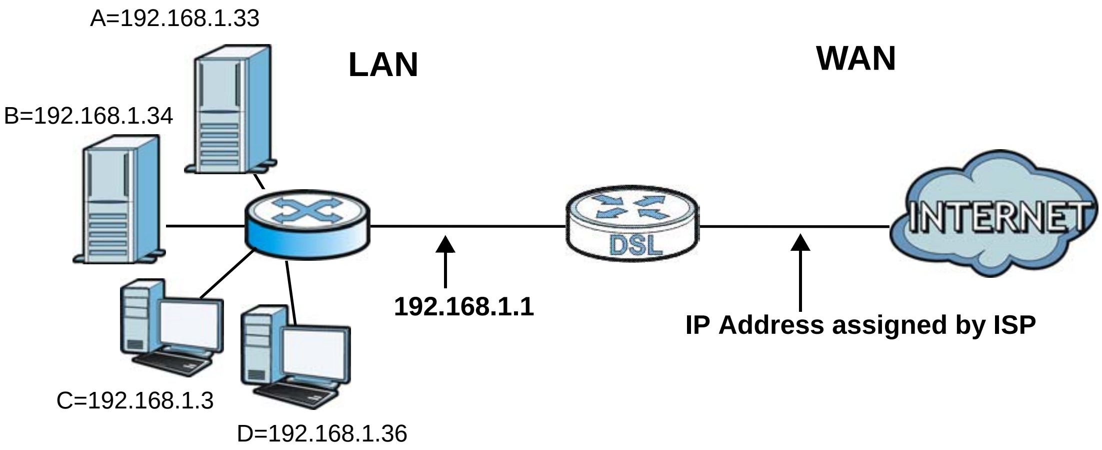
The most often used port numbers and services are shown in Appendix F on page 394. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

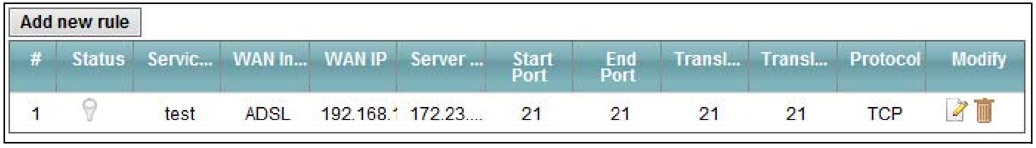
Figure 74 Multiple Servers Behind NAT Example



Click **Network Setting > NAT > Port Forwarding** to open the following screen.

See Appendix F on page 394 for port numbers commonly used for particular services.

Figure 75 Network Setting > NAT > Port Forwarding



Add new rule

#	Status	Servic...	WAN In...	WAN IP	Server ...	Start Port	End Port	Transl...	Transl...	Protocol	Modify
1	○	test	ADSL	192.168.1	172.23....	21	21	21	21	TCP	✎ 🗑

The following table describes the fields in this screen.

Table 53 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new rule.
#	This is the index number of the entry.
Status	This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This shows the service’s name.
WAN Interface	This shows the WAN interface through which the service is forwarded.
WAN IP	This field displays the incoming packet’s destination IP address.
Server IP Address	This is the server’s IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.

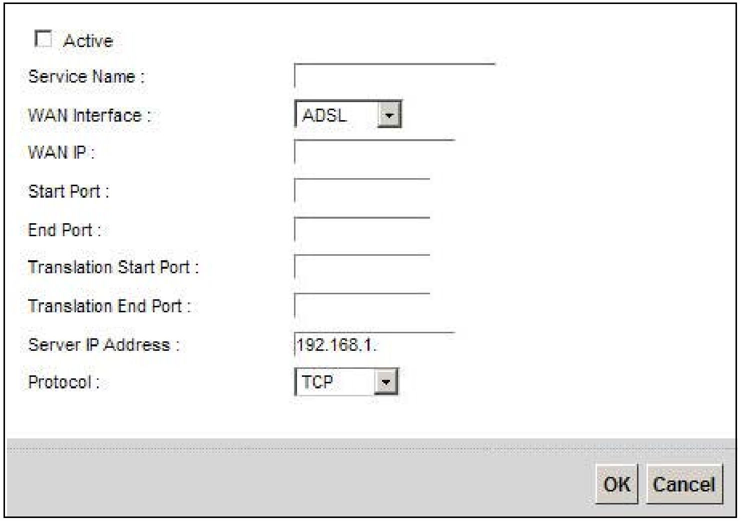
Table 53 Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Protocol	This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP / UDP**.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

11.2.1 Add/Edit Port Forwarding

Click **Add new rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen.

Figure 76 Port Forwarding: Add/Edit



☐ Active

Service Name :

WAN Interface : ADSL

WAN IP :

Start Port :

End Port :

Translation Start Port :

Translation End Port :

Server IP Address : 192.168.1.

Protocol : TCP

The following table describes the labels in this screen.

Table 54 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Clear the checkbox to disable the rule. Select the check box to enable it.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
WAN IP	Enter the WAN IP address for which the incoming service is destined. If the packet’s destination IP address doesn’t match the one specified here, the port forwarding rule will not be applied.
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.

Table 54 Port Forwarding: Add/Edit (continued)

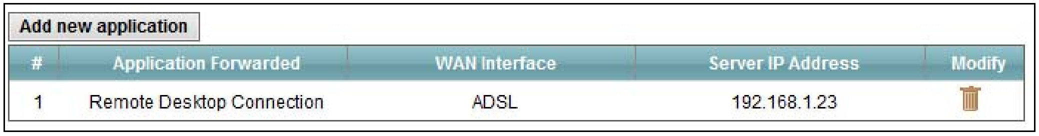
LABEL	DESCRIPTION
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Translation Start Port	This shows the port number to which you want the Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

11.3 The Applications Screen

This screen provides a summary of all NAT applications and their configuration. In addition, this screen allows you to create new applications and/or remove existing ones.

To access this screen, click **Network Setting > NAT > Applications**. The following screen appears.

Figure 77 Network Setting > NAT > Applications



Add new application

#	Application Forwarded	WAN Interface	Server IP Address	Modify
1	Remote Desktop Connection	ADSL	192.168.1.23	🗑

The following table describes the labels in this screen.

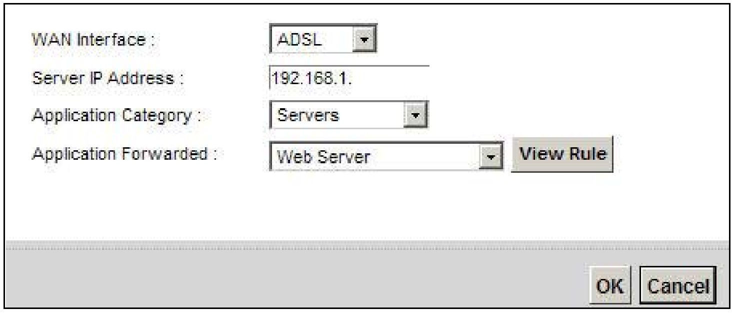
Table 55 Network Setting > NAT > Applications

LABEL	DESCRIPTION
Add new application	Click this to add a new NAT application rule.
#	This field displays the index number of the application rule.
Application Forwarded	This field shows the type of application that the service forwards.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Server IP Address	This field displays the destination IP address for the service.
Modify	Click the **Delete** icon to delete the rule.

11.3.1 Add New Application

This screen lets you create new NAT application rules. Click **Add new application** in the **Applications** screen to open the following screen.

Figure 78 Applications: Add



WAN Interface : ADSL

Server IP Address : 192.168.1.

Application Category : Servers

Application Forwarded : Web Server

The following table describes the labels in this screen.

Table 56 Applications: Add

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface that you want to apply this NAT rule to.
Server IP Address	Enter the inside IP address of the application here.
Application Category	Select the category of the application from the drop-down list box.
Application Forwarded	Select a service from the drop-down list box and the Device automatically configures the protocol, start, end, and map port number that define the service.
View Rule	Click this to display the configuration of the service that you have chosen in **Application Fowarded**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

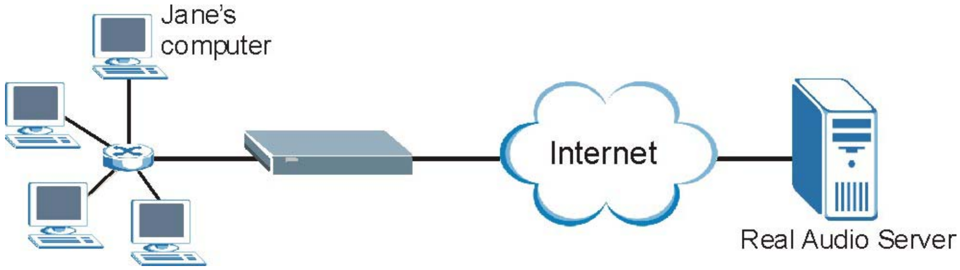
11.4 The Port Triggering Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Device's WAN port receives a response with a specific port number and protocol ("open" port), the Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 79 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the Device to record Jane's computer IP address. The Device associates Jane's computer IP address with the "open" port range of 6970-7170.

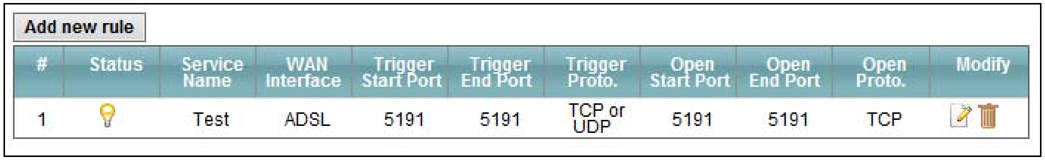
3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The Device forwards the traffic to Jane's computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your Device's trigger port settings.

Figure 80 Network Setting > NAT > Port Triggering



Add new rule

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Proto.	Modify
1	💡	Test	ADSL	5191	5191	TCP or UDP	5191	5191	TCP	✎ 🗑

The following table describes the labels in this screen.

Table 57 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.

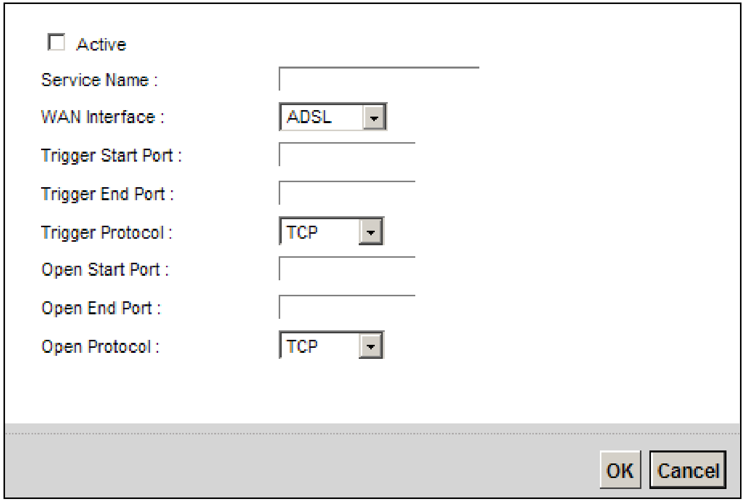
Table 57 Network Setting > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

11.4.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen.

Figure 81 Port Triggering: Add/Edit



□ Active

Service Name :	
WAN Interface :	ADSL
Trigger Start Port :	
Trigger End Port :	
Trigger Protocol :	TCP
Open Start Port :	
Open End Port :	
Open Protocol :	TCP

The following table describes the labels in this screen.

Table 58 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to enable this rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.

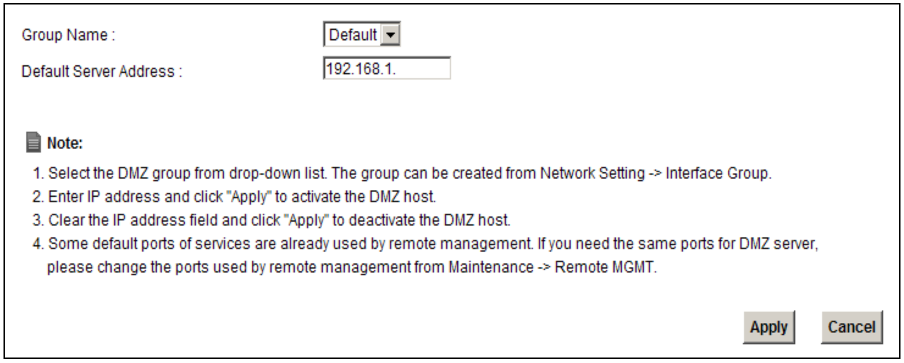
Table 58 Port Triggering: Configuration Add/Edit (continued)

LABEL	DESCRIPTION
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

11.5 The Default Server Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 82 Network Setting > NAT > Default Server



Group Name : Default

Default Server Address : 192.168.1.

Note:

1. Select the DMZ group from drop-down list. The group can be created from Network Setting -> Interface Group.
2. Enter IP address and click "Apply" to activate the DMZ host.
3. Clear the IP address field and click "Apply" to deactivate the DMZ host.
4. Some default ports of services are already used by remote management. If you need the same ports for DMZ server, please change the ports used by remote management from Maintenance -> Remote MGMT.

The following table describes the fields in this screen.

Table 59 Network Setting > NAT > Default Server

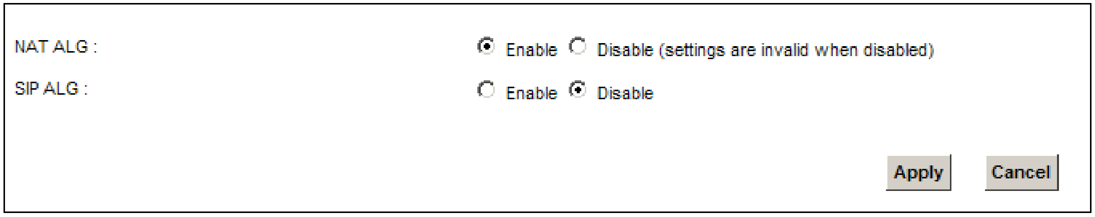
LABEL	DESCRIPTION
Group Name	Select the name of an interface group that was created in the **Network Setting** > **Interface Group** screen. The DMZ host must be in the same subnet as the selected interface group.
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server Address**, the Device discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

11.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Device registers with the SIP register server, the SIP ALG translates the Device’s private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Device is behind a SIP ALG.

Use this screen to enable and disable the NAT and SIP (VoIP) ALG in the Device. To access this screen, click **Network Setting > NAT > ALG**.

Figure 83 Network Setting > NAT > ALG



NAT ALG : ● Enable ○ Disable (settings are invalid when disabled)

SIP ALG : ○ Enable ● Disable

The following table describes the fields in this screen.

Table 60 Network Setting > NAT > ALG

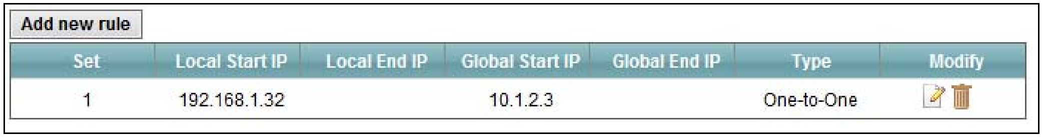
LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

11.7 The Address Mapping Screen

Ordering your rules is important because the Device applies the rules in the order that you specify. When a rule matches the current packet, the Device takes the corresponding action and the remaining rules are ignored.

Click **Network Setting > NAT > Address Mapping** to display the following screen.

Figure 84 Network Setting > NAT > Address Mapping



Set	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168.1.32		10.1.2.3		One-to-One	✎ 🗑

The following table describes the fields in this screen.

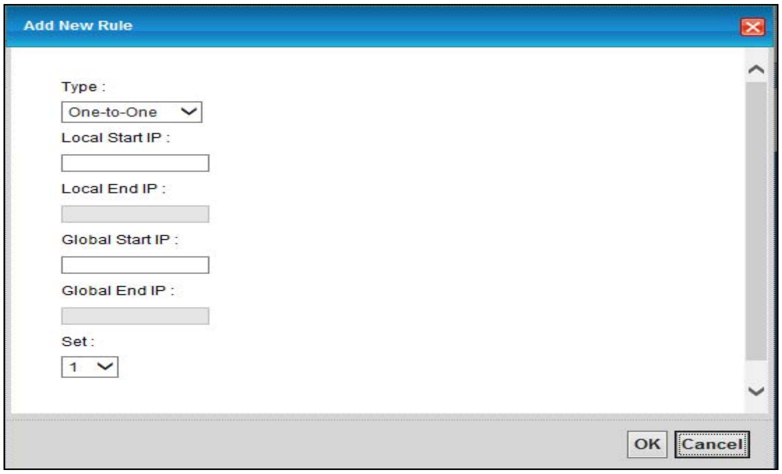
Table 61 Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
Set	This is the index number of the address mapping set.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
Type	This is the address mapping type. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Modify	Click the **Edit** icon to go to the screen where you can edit the address mapping rule. Click the **Delete** icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

11.7.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule’s edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 85 Address Mapping: Add/Edit



The following table describes the fields in this screen.

Table 62 Address Mapping: Add/Edit

LABEL	DESCRIPTION
Type	Choose the IP/port mapping type from one of the following. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
Set	Select the number of the mapping set for which you want to configure.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

11.8 Technical Reference

This part contains more information regarding NAT.

11.8.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 63 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

11.8.2 What NAT Does

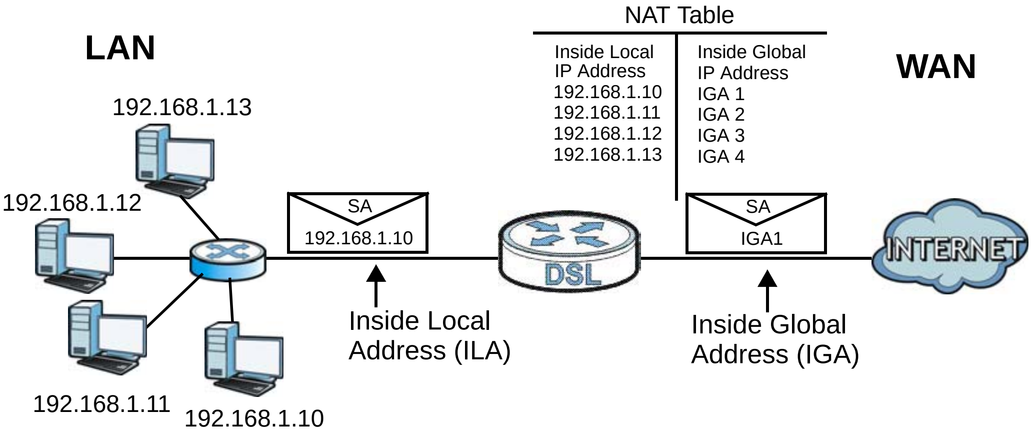
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, 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 (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

11.8.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 86 How NAT Works



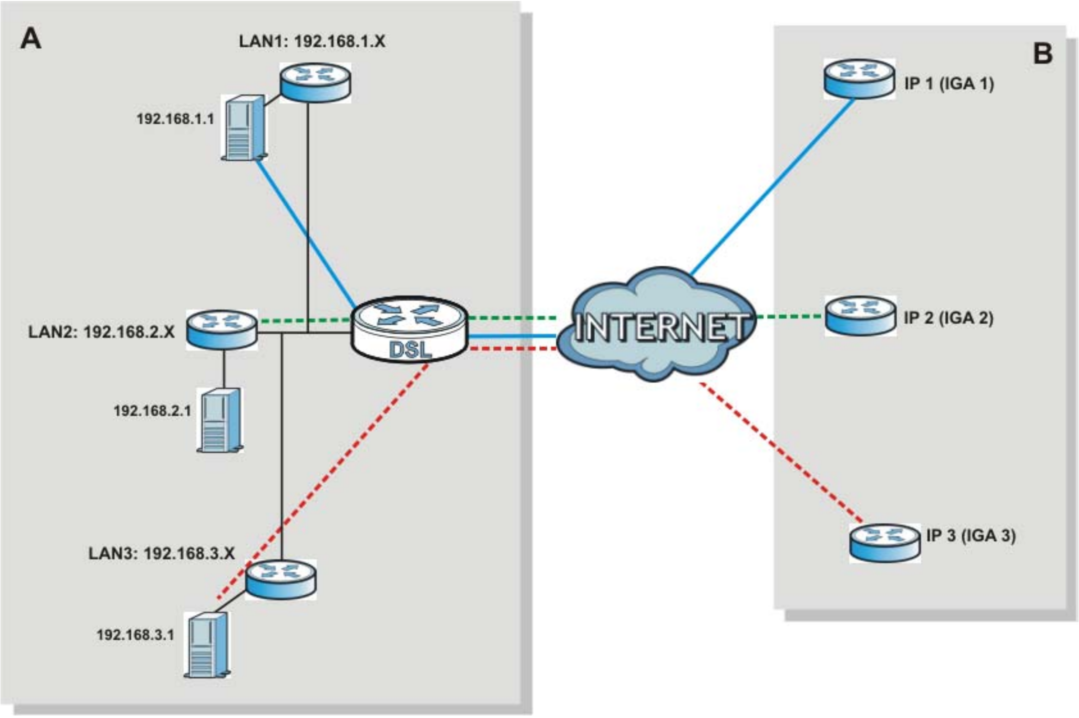
NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

11.8.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the Device can communicate with three distinct WAN networks.

Figure 87 NAT Application With IP Alias



Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

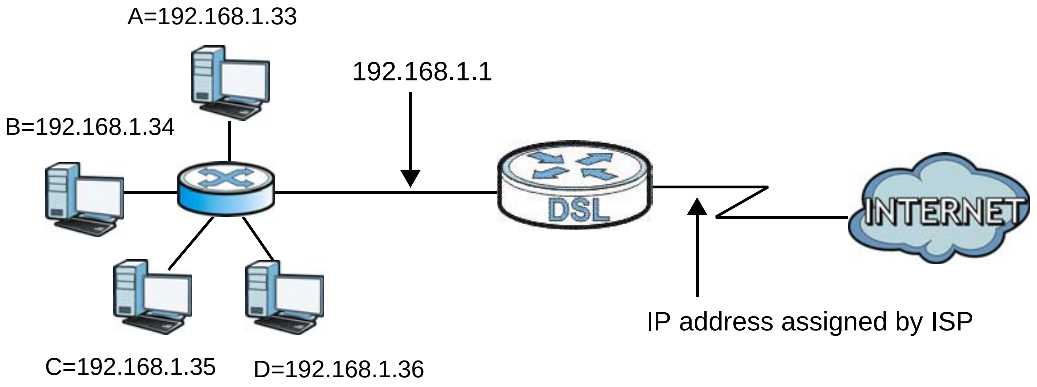
Table 64 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 88 Multiple Servers Behind NAT Example



Dynamic DNS Setup

12.1 Overview

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 12.2 on page 223).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Device (Section 12.3 on page 224).

12.1.2 What You Need To Know

DYNDNS Wildcard

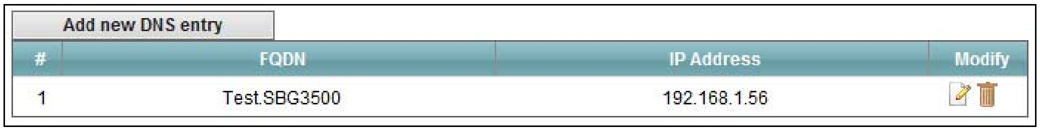
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 The DNS Entry Screen

Use this screen to view and configure DNS routes on the Device. Click **Network Setting > DNS** to open the **DNS Entry** screen.

Figure 89 Network Setting > DNS > DNS Entry



#	FQDN	IP Address	Modify
1	Test.SBG3500	192.168.1.56	✎ 🗑

The following table describes the fields in this screen.

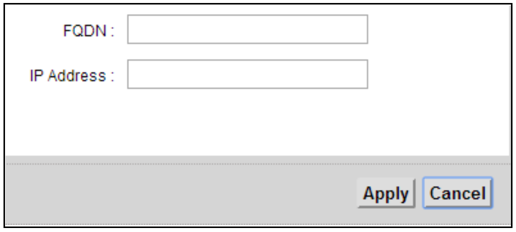
Table 65 Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add new DNS entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
Hostname	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule.

12.2.1 Add/Edit DNS Entry

You can manually add or edit the Device’s DNS name and IP address entry. Click **Add new DNS entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 90 DNS Entry: Add/Edit



The following table describes the labels in this screen.

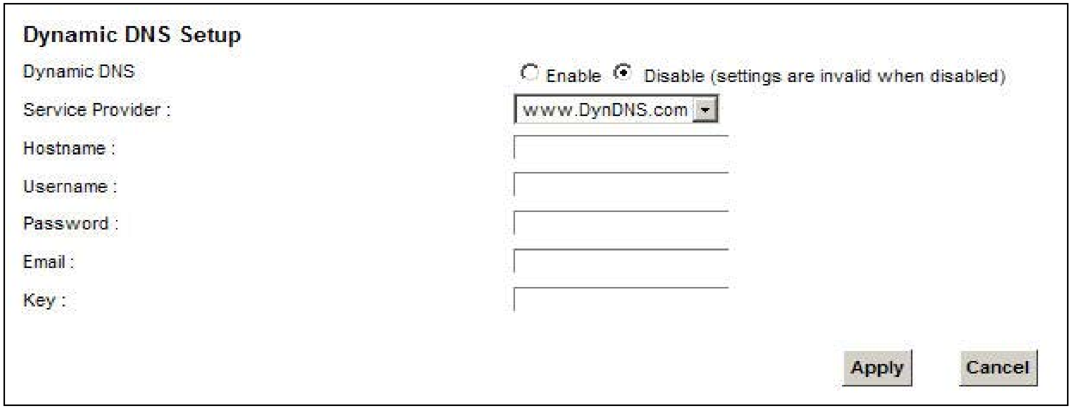
Table 66 DNS Entry: Add/Edit

LABEL	DESCRIPTION
FQDN	Enter the Fully Qualified Domain Name (FQDN) of the DNS entry. For example, if your hostname is myhost and a parent domain name is example.com, then your FQDN is myhost.example.com.
IP Address	Enter the IP address of the DNS entry.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

12.3 The Dynamic DNS Screen

Use this screen to change your Device's DDNS. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 91 Network Setting > DNS > Dynamic DNS



Dynamic DNS Setup

Dynamic DNS	○ Enable ● Disable (settings are invalid when disabled)
Service Provider :	www.DynDNS.com
Hostname :	
Username :	
Password :	
Email :	
Key :	

The following table describes the fields in this screen.

Table 67 Network Setting > DNS > > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Hostname	Type the domain name assigned to your Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Email	If you select **TZO** in the **Service Provider** field, enter the user name you used to register for this service.
Key	If you select **TZO** in the **Service Provider** field, enter the password you used to register for this service.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

13

Interface Group

13.1 Overview

By default, the four LAN interfaces on the Device are in the same group and can communicate with each other. Creating a new interface will create a new LAN bridge interface (subnet) (for example, 192.168.2.0/24) that acts as a dependent LAN network, and is a different subnet from default LAN subnet (192.168.1.0/24).

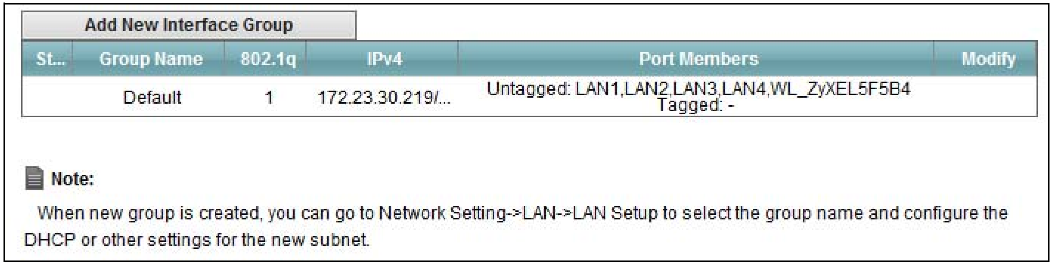
13.2 The Interface Group/VLAN Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the Device assigns to the clients in the default and/or user-defined groups. If you set the Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 8 on page 161 for more information.

Use the **Interface Group/VLAN** screen to create a new interface group, which is a new LAN bridge interface (subnet). Click **Network Setting > Interface Group/VLAN** to open the following screen.

Figure 92 Network Setting > Interface Group/VLAN



St...	Group Name	802.1q	IPv4	Port Members	Modify
	Default	1	172.23.30.219/...	Untagged: LAN1,LAN2,LAN3,LAN4,WL_ZyXEL5F5B4 Tagged: -	

Note:

When new group is created, you can go to Network Setting->LAN->LAN Setup to select the group name and configure the DHCP or other settings for the new subnet.

The following table describes the fields in this screen.

Table 68 Network Setting > Interface Group/VLAN

LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Status	This field displays whether the interface group is active or not. A yellow bulb signifies that this group is active. A gray bulb signifies that the group is not active.

Table 68 Network Setting > Interface Group/VLAN (continued)

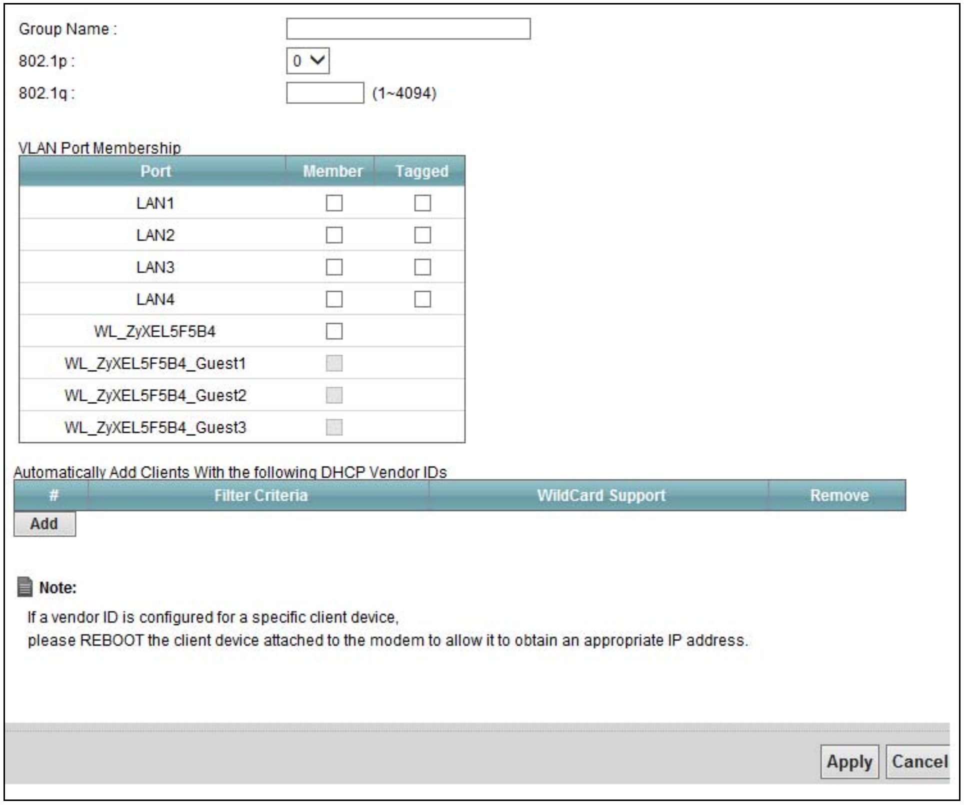
LABEL	DESCRIPTION
Group Name	This shows the descriptive name of the group.
802.1q	This shows the VLAN ID number (from 0 to 4094) of the interface group.
IPv4	This shows the IP address of the interface group where the traffic passes through.
Port Members	This shows the tagged and untagged ports of the interface group.
Modify	Click the **Delete** icon to remove the group.

13.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Group/VLAN** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to only one group at a time.

Figure 93 Interface Group Configuration



Group Name :

802.1p : 0

802.1q : (1~4094)

VLAN Port Membership

Port	Member	Tagged
LAN1	□	□
LAN2	□	□
LAN3	□	□
LAN4	□	□
WL_ZyXEL5F5B4	□	
WL_ZyXEL5F5B4_Guest1	□	
WL_ZyXEL5F5B4_Guest2	□	
WL_ZyXEL5F5B4_Guest3	□	

Automatically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Remove

Note:

If a vendor ID is configured for a specific client device,
please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

The following table describes the fields in this screen.

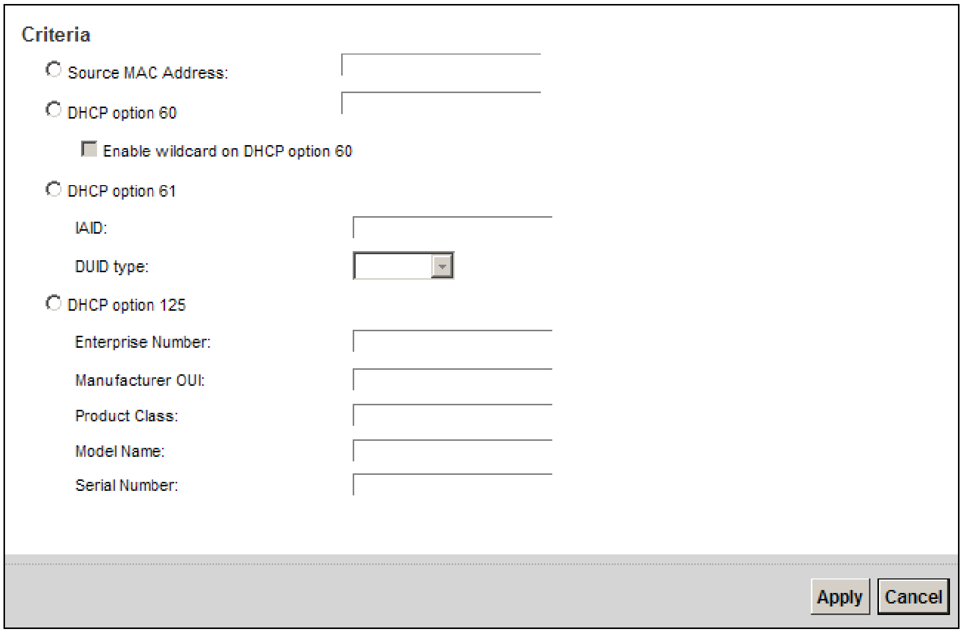
Table 69 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
VLAN Port Membership	
Port	This is the available LAN interface (Ethernet LAN or Wireless LAN) that can be selected to form a VLAN interface group.
Member	Click the check box to select the LAN port as a member of the VLAN interface group.
Tagged	Click the check box to set the port to tag or not to tag all outgoing traffic with the VLAN ID.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
WildCard Support	This shows if wildcard on DHCP option 60 is enabled.
Remove	Click the **Remove** icon to delete this rule from the Device.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to exit this screen without saving.

13.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen.

Figure 94 Interface Grouping Criteria



Criteria

○ Source MAC Address:

○ DHCP option 60

□ Enable wildcard on DHCP option 60

○ DHCP option 61

IAID:

DUID type:

○ DHCP option 125

Enterprise Number:

Manufacturer OUI:

Product Class:

Model Name:

Serial Number:

The following table describes the fields in this screen.

Table 70 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard on DHCP option 60 option	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID type	Select **DUID-LLT** (DUID Based on Link-layer Address Plus Time) to enter the hardware type, a time value and the MAC address of the device. Select **DUID-EN** (DUID Assigned by Vendor Based upon Enterprise Number) to enter the vendor’s registered enterprise number. Select **DUID-LL** (DUID Based on Link-layer Address) to enter the device’s hardware type and hardware address (MAC address) in the following fields. Select **Other** to enter any string that identifies the device in the DUID field.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.

Table 70 Interface Grouping Criteria (continued)

LABEL	DESCRIPTION
Enterprise Number	Enter the vendor’s 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor’s OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the device.
Model Name	Enter the model name of the device.
Serial Number	Enter the serial number of the device.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to exit this screen without saving.

14

USB Service

14.1 Overview

The Device has a USB port used to share files via a USB memory stick or a USB hard drive. In the **USB Service** screens, you can enable the file-sharing server.

14.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server (Section 14.2 on page 232).

14.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Device is given a folder, called a "share". If a USB hard drive connected to the Device has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems. It allows file and print sharing between computers running Windows and computers running Unix.

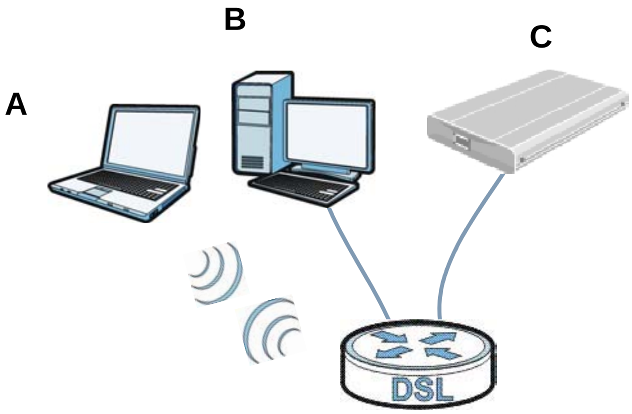
14.2 The File Sharing Screen

You can share files on a USB memory stick or hard drive connected to your Device with users on your network.

The Device supports Samba. This allows network users to access shared files in USB storage. To use file sharing you must enable it in the file sharing screen and also edit individual user accounts in the **Maintenance > User Account** screen. See Chapter 29 on page 300 for more information.

The following figure is an overview of the Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Device.

Figure 95 File Sharing Overview



The Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

14.2.1 Before You Begin

Make sure the Device is connected to your network and turned on.

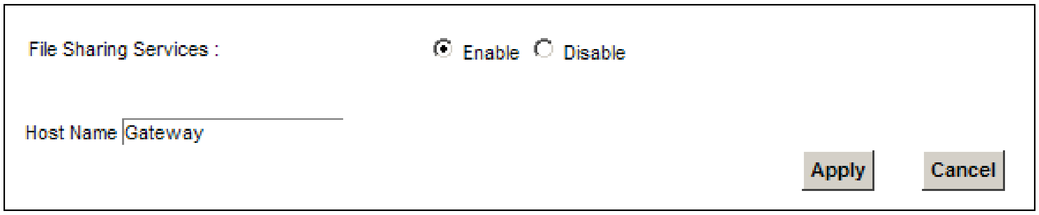
1 Connect the USB device to one of the Device's USB port. Make sure the Device is connected to your network.

2 The Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the Device, see the troubleshooting for suggestions.

Use this screen to set up file sharing using the Device. To access this screen, click **Network Setting > USB Service > File Sharing**.

Figure 96 Network Setting > USB Service > File Sharing



File Sharing Services : ● Enable ○ Disable

Host Name Gateway

Each field is described in the following table.

Table 71 Network Setting > LAN > File Sharing

LABEL	DESCRIPTION
File Sharing Services	Select **Enable** to activate file sharing through the Device.
Host Name	Enter the host name on the share.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

15

Firewall

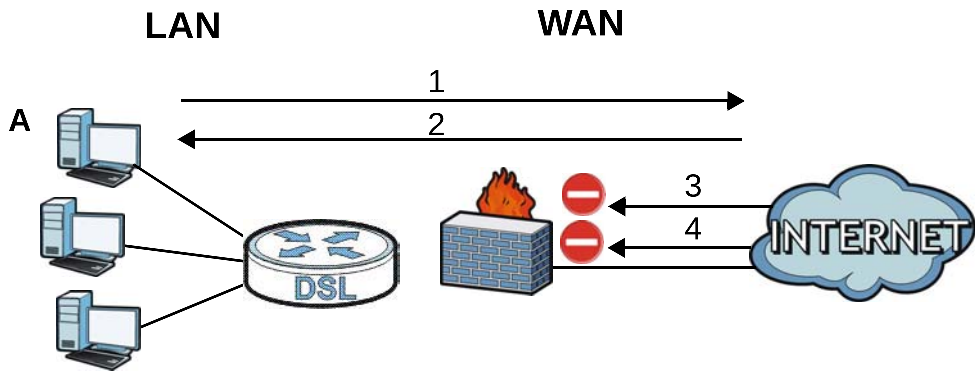
15.1 Overview

This chapter shows you how to enable and configure the SBG3500-N's security settings. Use the firewall to protect your SBG3500-N and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 97 Default Firewall Action



15.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the SBG3500-N (Section 15.2 on page 236).
- Use the **Service** screen to add or remove predefined Internet services and configure firewall rules (Section 15.3 on page 237).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 15.4 on page 239).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 15.5 on page 241).

15.1.2 What You Need to Know

SYN Attack

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

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

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

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

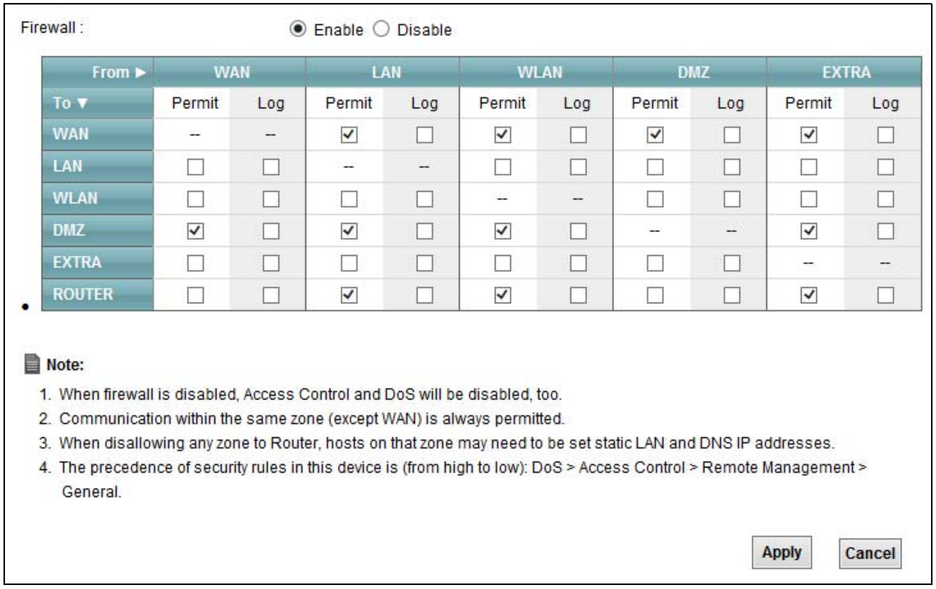
Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

15.2 The Firewall Screen

Use this screen to set the security level of the firewall on the SBG3500-N. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security > Firewall** to display the **General** screen.

Figure 98 Security > Firewall > General



Firewall : ● Enable ○ Disable

From ▶	WAN		LAN		WLAN		DMZ		EXTRA	
To ▼	Permit	Log	Permit	Log	Permit	Log	Permit	Log	Permit	Log
WAN	--	--	☑	□	☑	□	☑	□	☑	□
LAN	□	□	--	--	□	□	□	□	□	□
WLAN	□	□	□	□	--	--	□	□	□	□
DMZ	☑	□	☑	□	☑	□	--	--	☑	□
EXTRA	□	□	□	□	□	□	□	□	--	--
ROUTER	□	□	☑	□	☑	□	□	□	☑	□

Note:

1. When firewall is disabled, Access Control and DoS will be disabled, too.
2. Communication within the same zone (except WAN) is always permitted.
3. When disallowing any zone to Router, hosts on that zone may need to be set static LAN and DNS IP addresses.
4. The precedence of security rules in this device is (from high to low): DoS > Access Control > Remote Management > General.

The following table describes the labels in this screen.

Table 72 Security > Firewall > General

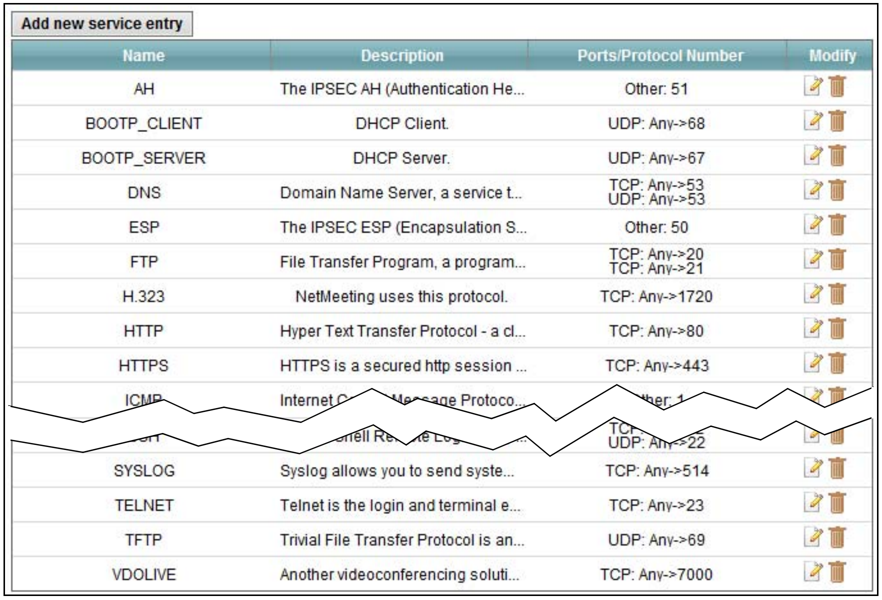
LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall feature on the SBG3500-N.
From/To	The firewall rules are grouped by the direction of packet travel and their zones (WAN, LAN, WLAN, DMZ, EXTRA and Router). By default, the firewall allows passage of packets traveling in the same zone (a LAN to a LAN, a WAN to a WAN). Here are some example descriptions of the directions of travel. **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the device. You can define the EXTRA zone to include the VPN connection. The Router zone can only be controlled in ingress direction "to" because it is reserved for the router's CPU. However, packets sent from the router zone are always permitted. For example, if your packet come from a LAN zone and is going to the Router zone. The SBG3500-N will apply the firewall rules to the LAN packets if you did not click the **Permit** check box. When **Permit** box is unchecked and **Log** box is checked, it means the "dropped" packets will be logged. When both Permit and Log boxes are checked, it means the "permitted" packets will be logged.
Permit	Click the check box **Permit** to allow the passage of the packets.
Log	Click the check box **Log** to create a log when an action from Firewall rule is taken.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

15.3 The Service Screen

You can configure customized services and port numbers in the **Service** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See Appendix F on page 394 for some examples.

Click **Security > Firewall > Service** to display the following screen.

Figure 99 Security > Firewall > Service



Add new service entry

Name	Description	Ports/Protocol Number	Modify
AH	The IPSEC AH (Authentication He...	Other: 51	✎ 🗑
BOOTP_CLIENT	DHCP Client.	UDP: Any->68	✎ 🗑
BOOTP_SERVER	DHCP Server.	UDP: Any->67	✎ 🗑
DNS	Domain Name Server, a service t...	TCP: Any->53 UDP: Any->53	✎ 🗑
ESP	The IPSEC ESP (Encapsulation S...	Other: 50	✎ 🗑
FTP	File Transfer Program, a program...	TCP: Any->20 TCP: Any->21	✎ 🗑
H.323	NetMeeting uses this protocol.	TCP: Any->1720	✎ 🗑
HTTP	Hyper Text Transfer Protocol - a cl...	TCP: Any->80	✎ 🗑
HTTPS	HTTPS is a secured http session ...	TCP: Any->443	✎ 🗑
ICMP	Internet C Message Protoco...	Other: 1	✎ 🗑
	Shell Re te Log ...	TCP: UDP: Any->22	✎ 🗑
SYSLOG	Syslog allows you to send syste...	TCP: Any->514	✎ 🗑
TELNET	Telnet is the login and terminal e...	TCP: Any->23	✎ 🗑
TFTP	Trivial File Transfer Protocol is an...	UDP: Any->69	✎ 🗑
VDOLIVE	Another videoconferencing soluti...	TCP: Any->7000	✎ 🗑

The following table describes the labels in this screen.

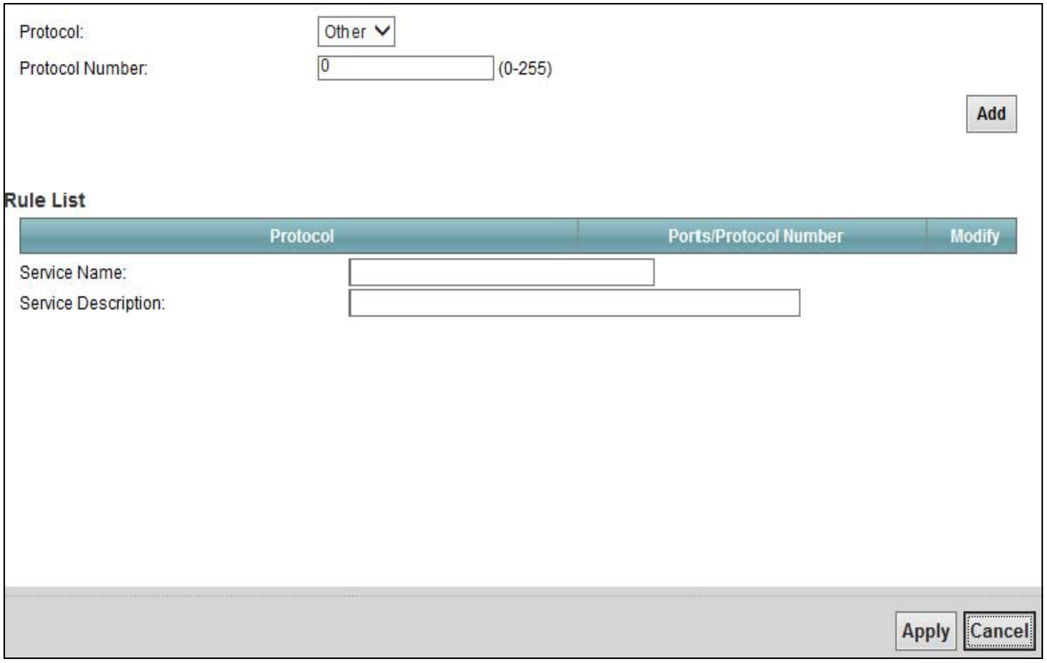
Table 73 Security > Firewall > Service

LABEL	DESCRIPTION
Add new service entry	Click this to add a new service.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Ports/Protocol Number	This shows the IP protocol (**TCP**, **UDP**, **ICMP**, or **TCP/UDP**) and the port number or range of ports that defines your customized service. **Other** and the protocol number displays if the service uses another IP protocol.
Modify	Click the **Edit** icon to edit the entry. Click the **Delete** icon to remove this entry.

15.3.1 Add/Edit a Service

Use this screen to add a customized service rule that you can use in the firewall’s ACL rule configuration. Click **Add new service entry** or the edit icon next to an existing service rule in the **Service** screen to display the following screen.

Figure 100 Service: Add/Edit



Protocol: Other

Protocol Number: 0 (0-255)

Rule List

Protocol	Ports/Protocol Number	Modify

Service Name:

Service Description:

The following table describes the labels in this screen.

Table 74 Service: Add/Edit

LABEL	DESCRIPTION
Protocol	Choose the IP protocol (**TCP**, **UDP**, **ICMP**, or **Other**) that defines your customized port from the drop-down list box. Select **Other** to be able to enter a protocol number.
Source/ Destination Port	These fields are displayed if you select **TCP** or **UDP** as the IP port. Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. If you select **Any**, the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
Protocol Number	This field is displayed if you select **Other** as the protocol. Enter the protocol number of your customized port.
Add	Click this to add the protocol to the **Rule List** below.
Rule List	
Protocol	This is the IP port (**TCP**, **UDP**, **ICMP**, or **Other**) that defines your customized port.
Ports/Protocol Number	For **TCP**, **UDP**, **ICMP**, or **TCP/UDP** protocol rules this shows the port number or range that defines the custom service. For other IP protocol rules this shows the protocol number.
Modify	Click the **Delete** icon to remove the rule.
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.

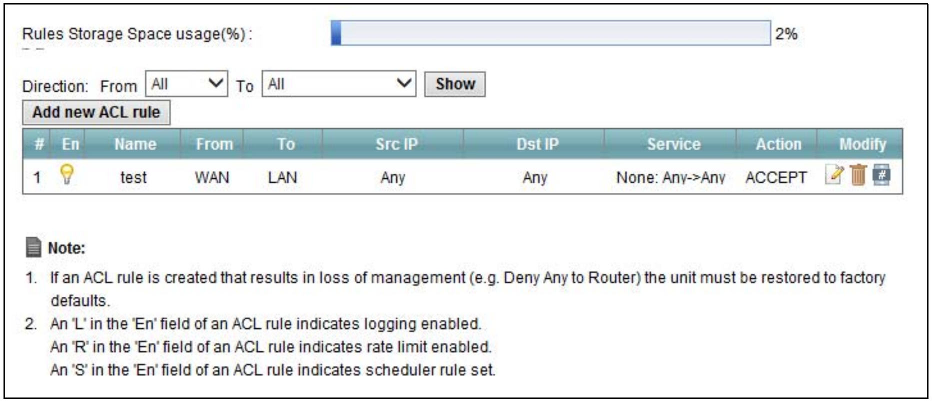
Table 74 Service: Add/Edit (continued)

LABEL	DESCRIPTION
Service Description	Enter a description for your customized port.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

15.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 101 Security > Firewall > Access Control



Rules Storage Space usage(%) : 2%

Direction: From All To All

#	En	Name	From	To	Src IP	Dst IP	Service	Action	Modify
1	💡	test	WAN	LAN	Any	Any	None: Any->Any	ACCEPT	

Note:

1. If an ACL rule is created that results in loss of management (e.g. Deny Any to Router) the unit must be restored to factory defaults.
2. An 'L' in the 'En' field of an ACL rule indicates logging enabled.
   An 'R' in the 'En' field of an ACL rule indicates rate limit enabled.
   An 'S' in the 'En' field of an ACL rule indicates scheduler rule set.

The following table describes the labels in this screen.

Table 75 Security > Firewall > Access Control

LABEL	DESCRIPTION
Rules Storage Space usage	This bar shows the percentage of the SBG3500-N’s space has been used. If the usage is almost full, you may need to remove an existing filter rule before you create a new one.
Direction	This displays the direction of the ACL rule.
Add new ACL rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
#	This is the index number of the entry.
Enable	This field displays whether the ACL rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Name	This displays the name of the rule.
From/To	This is the packet direction. Choose the interfaces from the drop-down list to set the direction of the packet that the ACL rule applies.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.

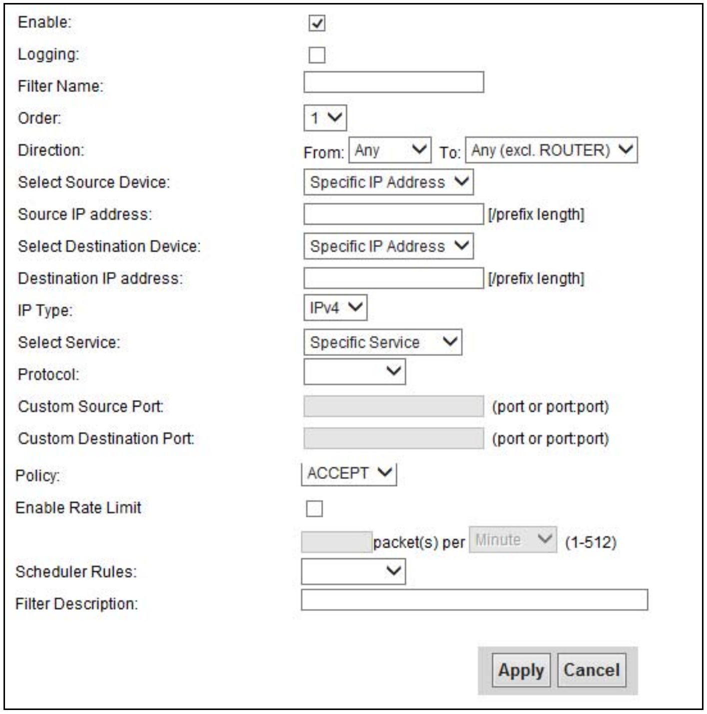
Table 75 Security > Firewall > Access Control (continued)

LABEL	DESCRIPTION
Action	This is the policy of the access control. Choose the following option from the drop-down list: Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Accept** to allow the passage of the packets.
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action. Click the **Move To** icon to change the order of the rule. Enter the number in the # field.

15.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 102 Access Control: Add/Edit



Enable:	☑
Logging:	□
Filter Name:	
Order:	1
Direction:	From: Any To: Any (excl. ROUTER)
Select Source Device:	Specific IP Address
Source IP address:	[/prefix length]
Select Destination Device:	Specific IP Address
Destination IP address:	[/prefix length]
IP Type:	IPv4
Select Service:	Specific Service
Protocol:	
Custom Source Port:	(port or port:port)
Custom Destination Port:	(port or port:port)
Policy:	ACCEPT
Enable Rate Limit	□
	packet(s) per Minute (1-512)
Scheduler Rules:	
Filter Description:	

The following table describes the labels in this screen.

Table 76 Access Control: Add/Edit

LABEL	DESCRIPTION
Enable	Click the check box to activate the ACL.
Logging	Click the check box if you want to log the packet throughput in this ACL.
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.

Table 76 Access Control: Add/Edit (continued)

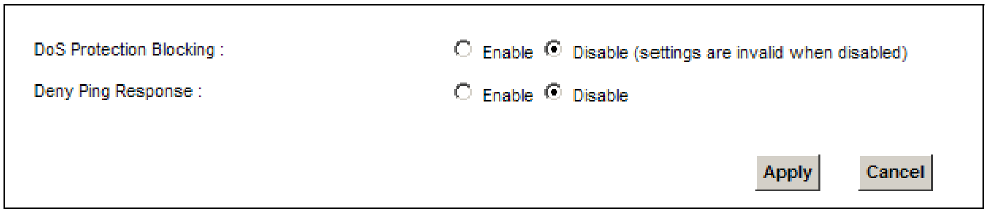
LABEL	DESCRIPTION
Order	Select the order of the ACL rule.
Direction	Select the direction of the ACL rule. You may select from **WAN to LAN**, **WAN to Router**, **WAN to DMZ**, **LAN to WAN**, **LAN to Router**, **LAN to DMZ**, **DMZ to WAN**, **DMZ to LAN**, and **DMZ to Router**. The DMZ zone is available when there's a specified DMZ group.
Select Source Device	Select the source device to which the ACL rule applies. If you select **Specific IP Address**, enter the source IP address in the field below.
Source IP Address	Enter the source IP address.
Select Destination DevicSBG3500-Ne	Select the destination device to which the ACL rule applies. If you select **Specific IP Address**, enter the destiniation IP address in the field below.
Destination IP Address	Enter the destination IP address.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Select Service	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the **Security > Firewall > Service > Add** screen display in this list. If you want to configure a customized protocol, select **Specific Service**.
Protocol	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Choose the IP port (**TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) that defines your customized port from the drop-down list box.
Custom Source Port	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the destination.
Policy	Use the drop-down list box to select whether to discard (**DROP**), deny and send an ICMP destination-unreachable message to the sender of (**REJECT**) or allow the passage of (**ACCEPT**) packets that match this rule.
Enable Rate Limit	Select this check box to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click **Add New Rule**. This will bring you to the **Security > Scheduler Rules** screen.
Filter Description	Type a description of the Filter of this ACL rule. This field is optional.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

15.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 103 Security > Firewall > DoS



DoS Protection Blocking : ○ Enable ● Disable (settings are invalid when disabled)

Deny Ping Response : ○ Enable ● Disable

The following table describes the labels in this screen.

Table 77 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select **Enable** to enable protection against DoS attacks.
Deny Ping Response	Select Enable to block ping request packets.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

MAC Filter

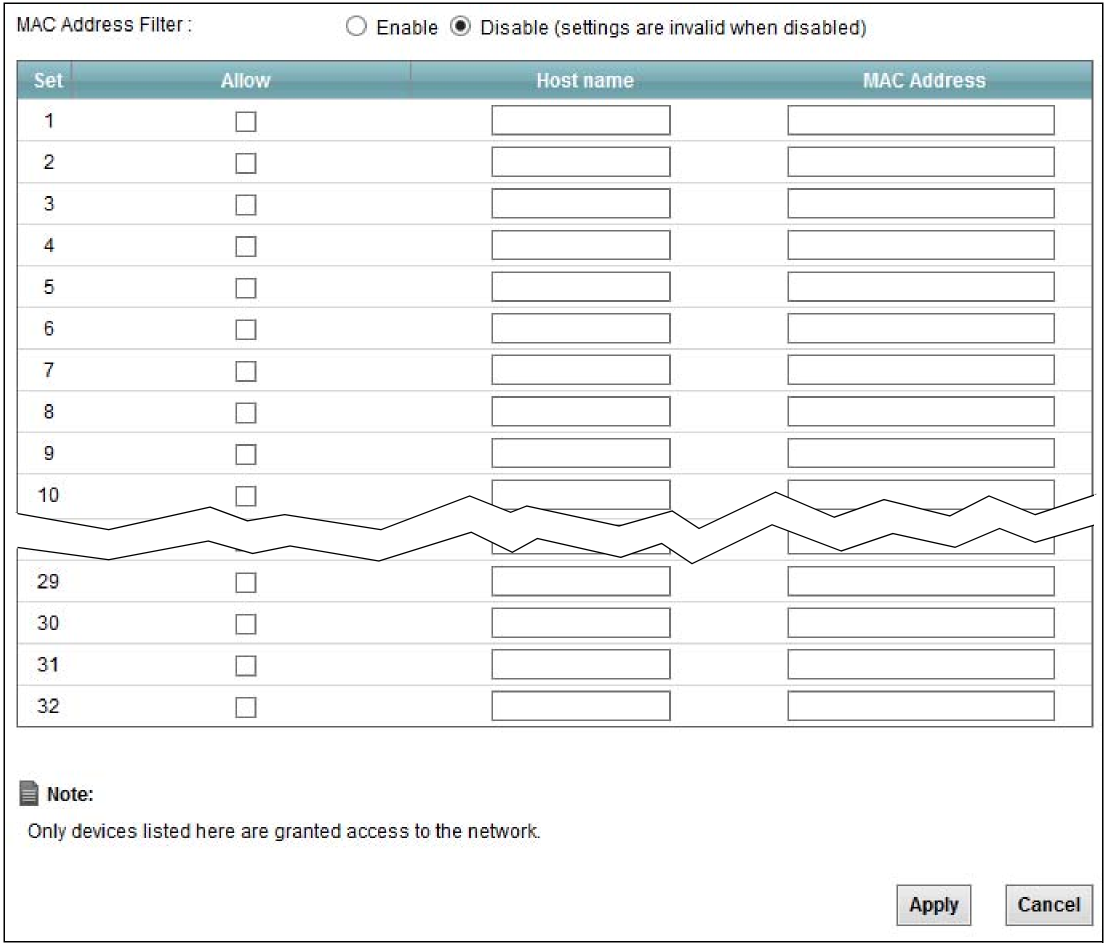
16.1 Overview

You can configure the Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

16.2 The MAC Filter Screen

Use this screen to allow wireless and LAN clients access to the Device. Click **Security** > **MAC Filter**. The screen appears as shown.

Figure 104 Security > MAC Filter



MAC Address Filter : ○ Enable ● Disable (settings are invalid when disabled)

Set	Allow	Host name	MAC Address
1	□		
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		
9	□		
10	□		
29	□		
30	□		
31	□		
32	□		

Note:

Only devices listed here are granted access to the network.

The following table describes the labels in this screen.

Table 78 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate the MAC filter function.
Set	This is the index number of the MAC address.
Allow	Select **Allow** to permit access to the Device. MAC addresses not listed will be denied access to the Device. If you clear this, the MAC Address field for this set clears.
Host name	Enter the host name of the wireless or LAN clients that are allowed access to the Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

17

User Access Control

17.1 Overview

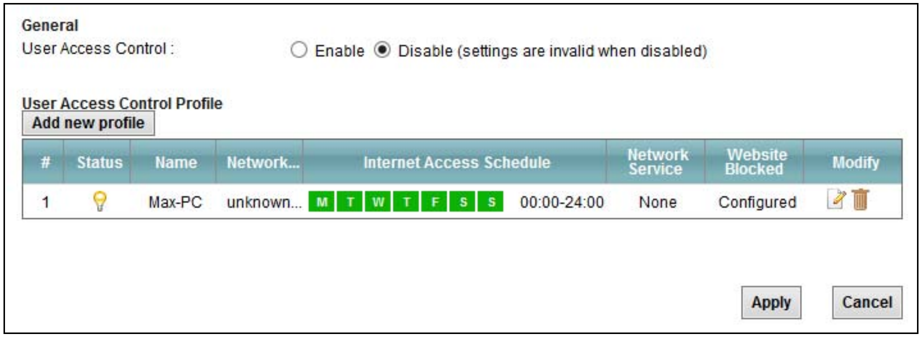
User Access control allows you to block web sites with the specific URL. You can also define time periods and days during which the Device performs User Access control on a specific user.

17.2 The User Access Control Screen

Use this screen to enable User Access control, view the User Access control rules and schedules.

Click **Security** > **User Access Control** to open the following screen.

Figure 105 Security > User Access Control



General

User Access Control : ○ Enable ● Disable (settings are invalid when disabled)

User Access Control Profile

Add new profile

#	Status	Name	Network...	Internet Access Schedule	Network Service	Website Blocked	Modify
1	💡	Max-PC	unknown...	M T W T F S S 00:00-24:00	None	Configured	✎ 🗑

The following table describes the fields in this screen.

Table 79 Security > User Access Control

LABEL	DESCRIPTION
User Access Control	Select **Enable** to activate User Access control.
Add new profile	Click this if you want to configure a new User Access control rule.
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Name	This shows the name of the rule.
Network User (MAC)	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which User Access control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.

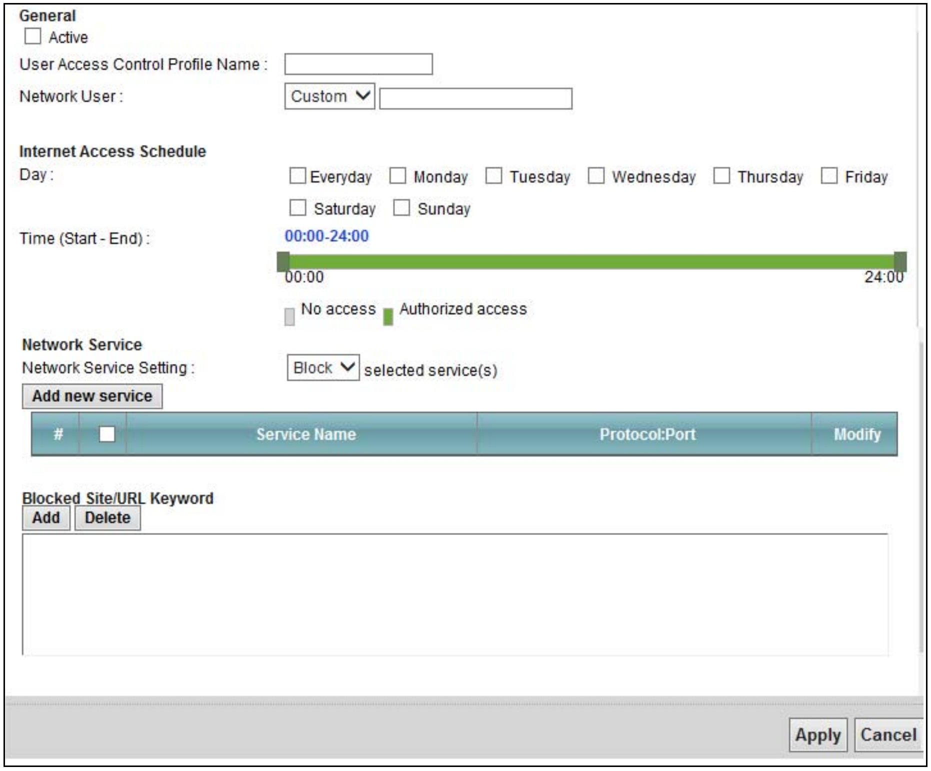
Table 79 Security > User Access Control (continued)

LABEL	DESCRIPTION
Website Block	This shows whether the website block is configured. If not, **None** will be shown.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

17.2.1 Add/Edit a User Access Control Rule

Click **Add new profile** in the **User Access Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 106 User Access Control Rule: Add/Edit



General

□ Active

User Access Control Profile Name :

Network User : Custom

Internet Access Schedule

Day : □ Everyday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Time (Start - End) : 00:00-24:00

Network Service

Network Service Setting : Block selected service(s)

#	□	Service Name	Protocol:Port	Modify

Blocked Site/URL Keyword

The following table describes the fields in this screen.

Table 80 User Access Control Rule: Add/Edit

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate this User Access control rule.
User Access Control Profile Name	Enter a descriptive name for the rule.

Table 80 User Access Control Rule: Add/Edit (continued)

LABEL	DESCRIPTION
Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Device to perform User Access control.
Time	Drag the time bar to define the time that the LAN user is allowed access.
Network Service	
Network Service Setting	If you select **Block**, the Device prohibits the users from viewing the Web sites with the URLs listed below. If you select **Allow**, the Device blocks access to all URLs except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Name** of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the **Edit** icon to go to the screen where you can edit the rule. Click the **Delete** icon to delete an existing rule.
Blocked Site/ URL Keyword	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the Device blocks access. Click **Delete** to remove it.
Apply	Click this button to save your settings back to the Device.
Cancel	Click **Cancel** to restore your previously saved settings.

18

Scheduler Rules

18.1 Overview

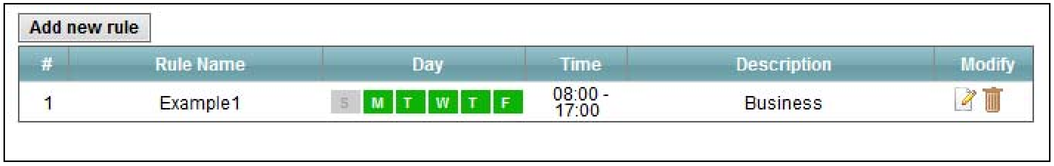
You can define time periods and days during which the Device performs scheduled rules of certain features (such as Firewall Access Control, User Access Control) on a specific user in the **Scheduler Rules** screen.

18.2 The Scheduler Rules Screen

Use this screen to view, add, or edit time schedule rules.

Click **Security > Scheduler Rules** to open the following screen.

Figure 107 Security > Scheduler Rules



Add new rule

#	Rule Name	Day	Time	Description	Modify
1	Example1	S M T W T F	08:00 - 17:00	Business	

The following table describes the fields in this screen.

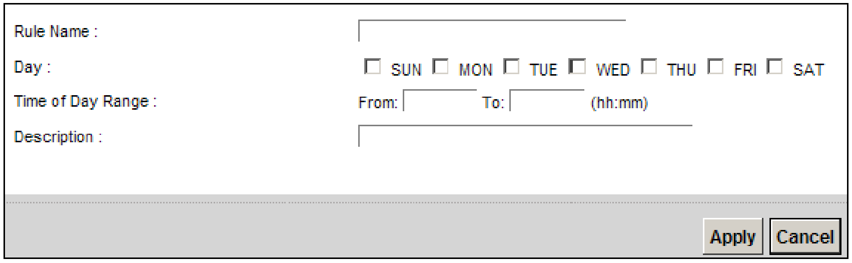
Table 81 Security > Scheduler Rules

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the **Edit** icon to edit the schedule. Click the **Delete** icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

18.2.1 Add/Edit a Schedule

Click the **Add** button in the **Scheduler Rules** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule for a specific user on your network.

Figure 108 Scheduler Rules: Add/Edit



Rule Name :	
Day :	□ SUN □ MON □ TUE □ WED □ THU □ FRI □ SAT
Time of Day Range :	From: To: (hh:mm)
Description :	

The following table describes the fields in this screen.

Table 82 Scheduler Rules: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the Device to perform this scheduler rule.
Time if Day Range	Enter the time period of each day, in 24-hour format, during which User Access control will be enforced.
Description	Enter a description for this scheduler rule.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

19

Certificates

19.1 Overview

The Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

19.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the Device's CA-signed certificates (Section 19.4 on page 254).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Device (Section 19.4 on page 254).

19.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

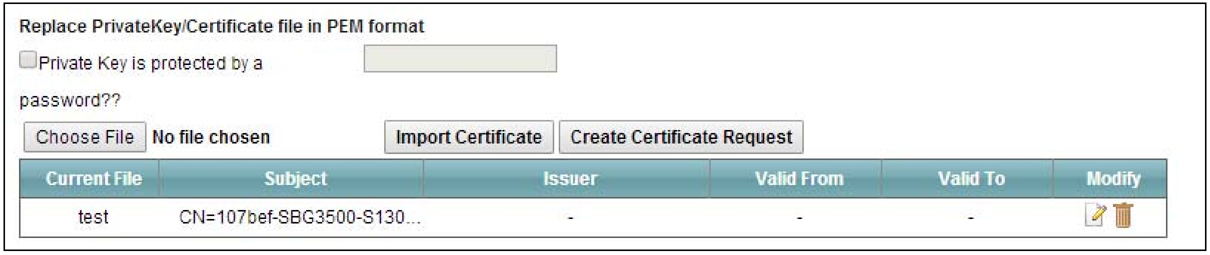
Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

19.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the Device's summary list of certificates and certification requests.

Figure 109 Security > Certificates > Local Certificates



Replace PrivateKey/Certificate file in PEM format

□Private Key is protected by a password??

Current File	Subject	Issuer	Valid From	Valid To	Modify
test	CN=107bef-SBG3500-S130...	-	-	-	

The following table describes the labels in this screen.

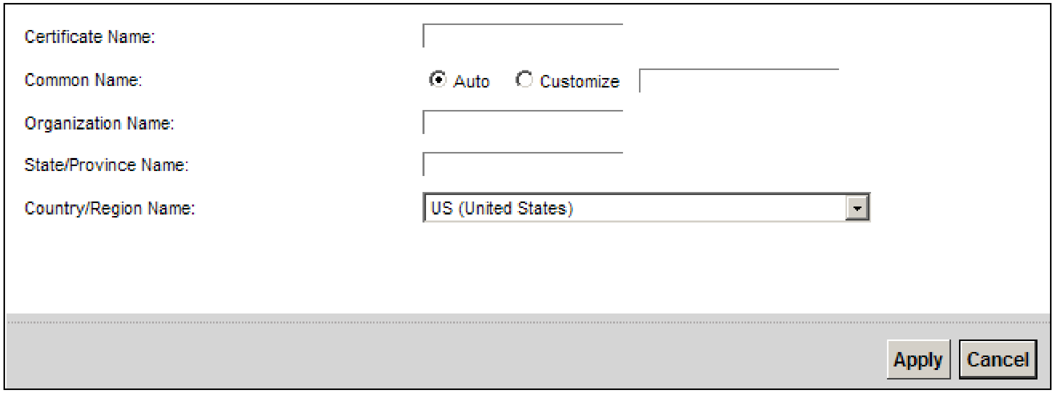
Table 83 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Private Key is protected by a password?	Select the checkbox and enter the private key into the text box to store it on the Device. The private key should not exceed 63 ASCII characters (not including spaces).
Browse...	Click this to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Device.
Create Certificate Request	Click this button to go to the screen where you can have the Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

19.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Device generate a certification request.

Figure 110 Create Certificate Request



Certificate Name:

Common Name: ● Auto ○ Customize

Organization Name:

State/Province Name:

Country/Region Name: US (United States)

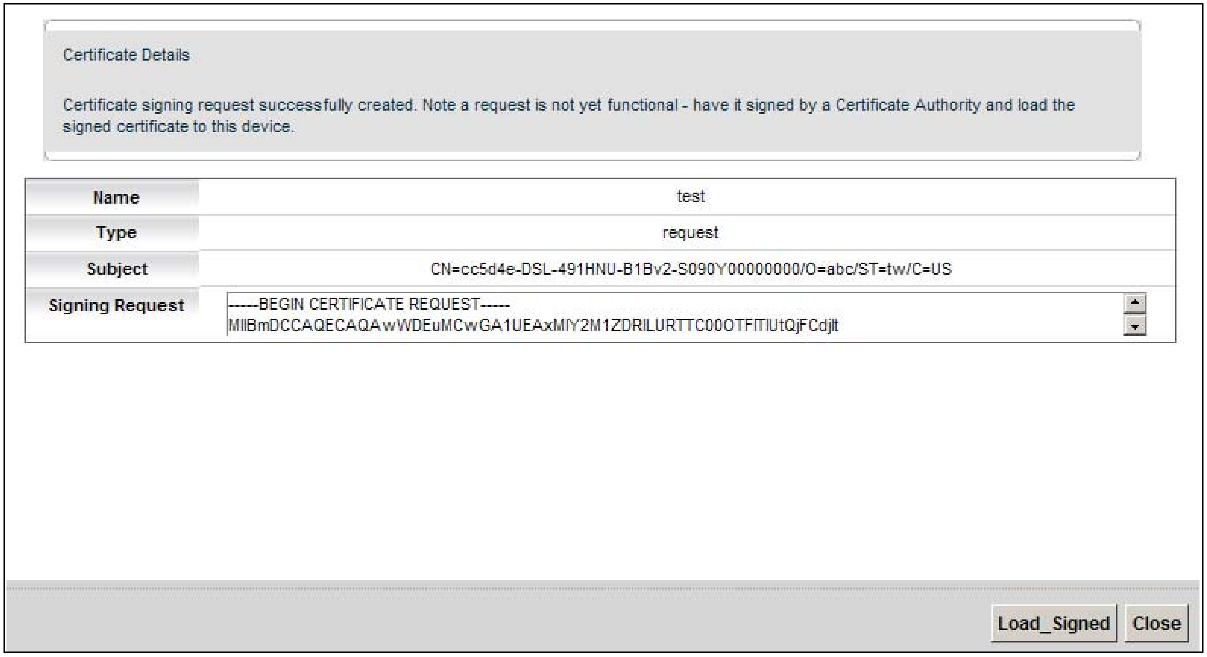
The following table describes the labels in this screen.

Table 84 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the Device configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

After you click **Apply**, the following screen displays to notify you that you need to get the certificate request signed by a Certificate Authority. If you already have, click **Load_Signed** to import the signed certificate into the Device. Otherwise click **Back** to return to the **Local Certificates** screen.

Figure 111 Certificate Request Created



Certificate Details

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

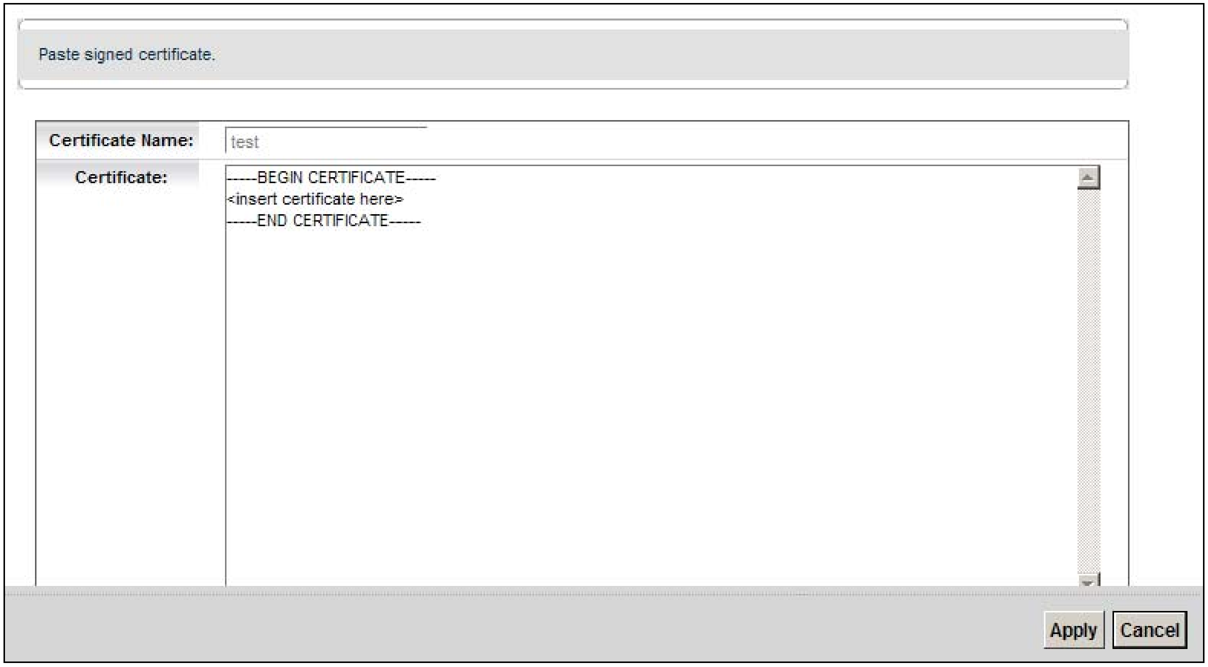
Name	test
Type	request
Subject	CN=cc5d4e-DSL-491HNU-B1Bv2-S090Y00000000/O=abc/ST=tw/C=US
Signing Request	-----BEGIN CERTIFICATE REQUEST----- MIIBmDCCAQECAQAwWDEuMCwGA1UEAxMIY2M1ZDRILURTTC00OTFITlUtQjFCdjlt

19.3.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **Local Certificates** screen click the certificate request’s **Load Signed** icon to import the signed certificate into the Device.

Note: You must remove any spaces from the certificate’s filename before you can import it.

Figure 112 Load Signed Certificate



Paste signed certificate.

Certificate Name:	test
Certificate:	-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----

The following table describes the labels in this screen.

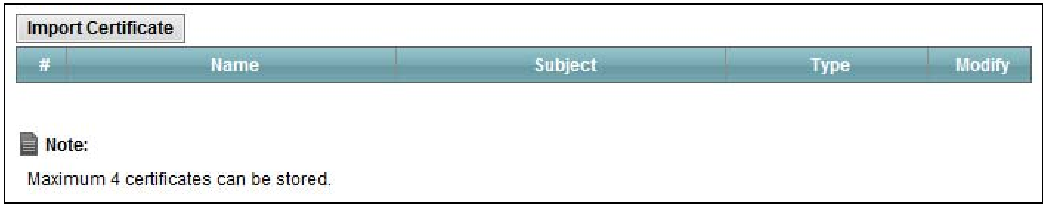
Table 85 Load Signed Certificate

LABEL	DESCRIPTION
Certificate Name	This is the name of the signed certificate.
Certificate	Copy and paste the signed certificate into the text box to store it on the Device.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

19.4 The Trusted CA Screen

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the Device to accept as trusted. The Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 113 Security > Certificates > Trusted CA



Note:

Maximum 4 certificates can be stored.

The following table describes the fields in this screen.

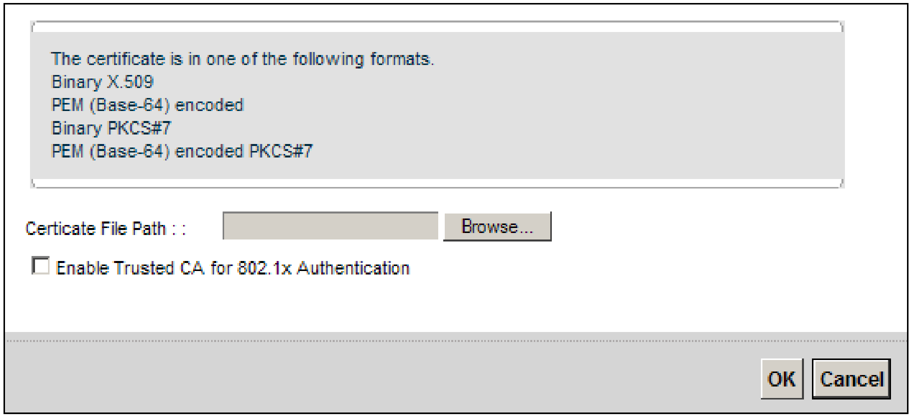
Table 86 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

19.4.1 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The Device trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 114 Trusted CA: Import Certificate



The certificate is in one of the following formats.
Binary X.509
PEM (Base-64) encoded
Binary PKCS#7
PEM (Base-64) encoded PKCS#7

Certicate File Path : :

□ Enable Trusted CA for 802.1x Authentication

The following table describes the fields in this screen.

Table 87 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the certificate you want to upload in this field or click **Browse ...** to find it.
Enable Trusted CA for 802.1x Authentication	If you select this checkbox, the trusted CA will be used for 802.1x authentication. The selected trusted CA will be displayed in the **Network Setting** > **Broadband** > **802.1x: Edit** screen.
Certificate	Copy and paste the certificate into the text box to store it on the Device.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

20

IPSec VPN

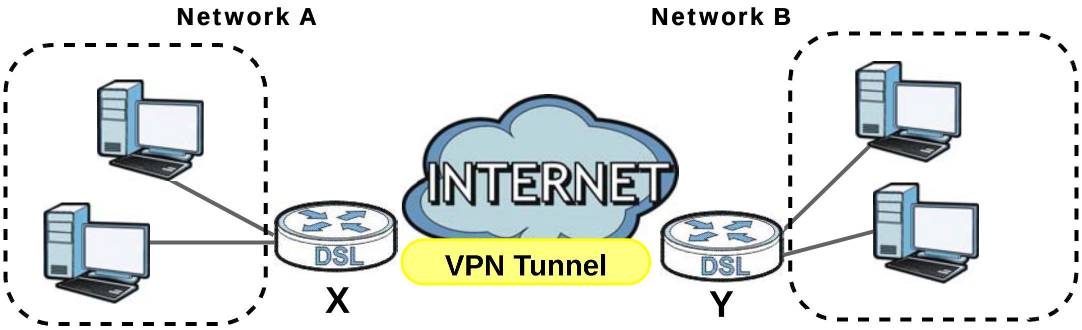
20.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure provides one perspective of a VPN tunnel.

Figure 115 IPSec VPN: Overview



The VPN tunnel connects the SBG3500-N (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

20.2 What You Can Do in this Chapter

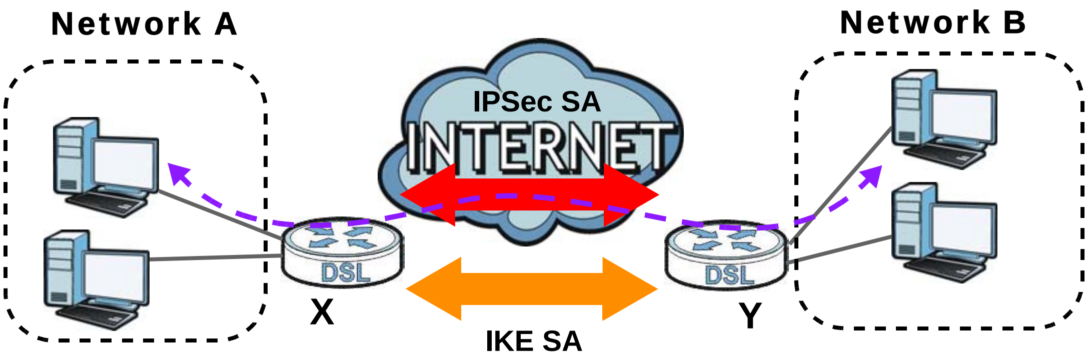
- Use the **Setup** screen to display and manage the SBG3500-N's IPSec VPN rules (tunnels) (Section 20.4 on page 257).
- Use the **Monitor** screen to display and manage active IPSec VPN connections (Section 20.5 on page 266).
- Use the **Radius** screen to manage the list of RADIUS servers the SBG3500-N can use in authenticating users (Section 20.6 on page 267).

20.3 What You Need To Know

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the SBG3500-N and the remote IPSec router will use.

The first phase establishes an Internet Key Exchange (IKE) SA between the SBG3500-N and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the SBG3500-N and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 116 VPN: IKE SA and IPSec SA

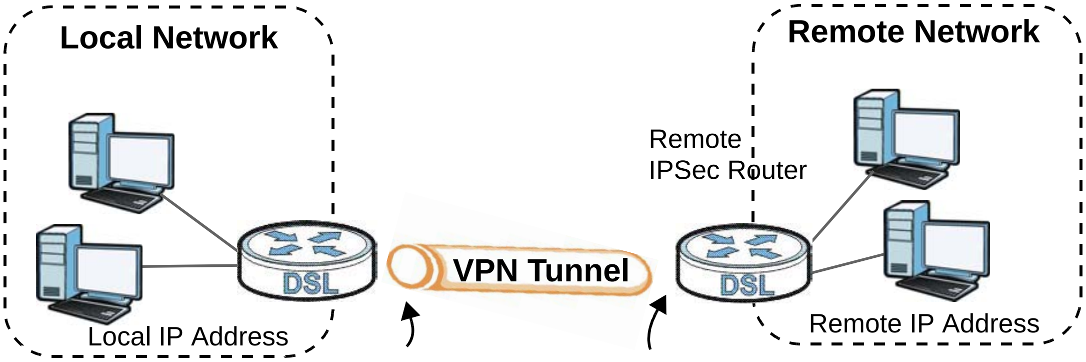


In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

20.4 The Setup Screen

The following figure helps explain the main fields in the web configurator.

Figure 117 IPSec Fields Summary

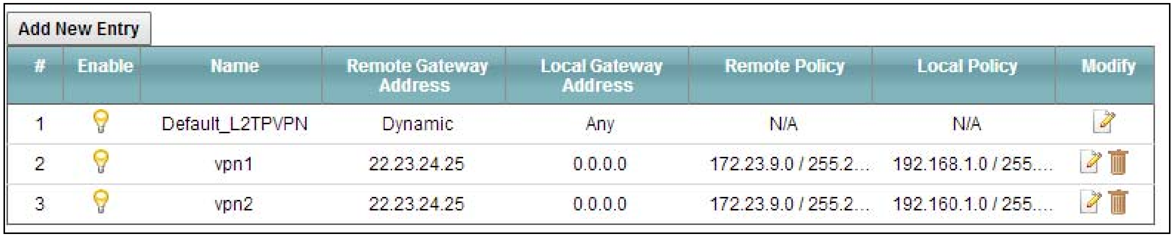


Local and remote IP addresses must be static.

Click **VPN > IPSec VPN** to display the **Setup** screen. This is a read-only menu of your IPSec VPN rules (tunnels). Edit a VPN rule by clicking the **Edit** icon.

Note: The default IPsec rule **Default_L2TPVPN** cannot be disconnected on the **VPN** > **IPSec VPN > Monitor** screen. However, you may disconnect L2TP tunnels in the **VPN** > **L2TP** > **Monitor** screen.

Figure 118 VPN > IPSec VPN > Setup



#	Enable	Name	Remote Gateway Address	Local Gateway Address	Remote Policy	Local Policy	Modify
1	●	Default_L2TPVPN	Dynamic	Any	N/A	N/A	✎
2	●	vpn1	22.23.24.25	0.0.0.0	172.23.9.0 / 255.2...	192.168.1.0 / 255....	✎ 🗑
3	●	vpn2	22.23.24.25	0.0.0.0	172.23.9.0 / 255.2...	192.160.1.0 / 255....	✎ 🗑

The following table describes the fields in this screen.

Table 88 VPN > IPSec VPN > Setup

LABEL	DESCRIPTION
Add New Entry	Click this button to set up VPN policies for a new tunnel.
#	This is the VPN policy index number.
Enable	This field displays whether the VPN policy is active or not. This icon is turned on when the rule is enabled.
Name	This field displays the identification name for this VPN policy.
Remote Gateway Address	This field displays the Secure Gateway Address of the IPSec router with which you're making the VPN connection.
Local Gateway Address	This field displays the IP address used by the SBG3500-N. If the selected interface is not available, this field will display 0.0.0.0.
Remote Policy	This field displays the remote policy.
Local Policy	This field displays the local policy.
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN rule. Click the **Remove** icon to remove an existing VPN rule.

20.4.1 Add/Edit VPN Rule

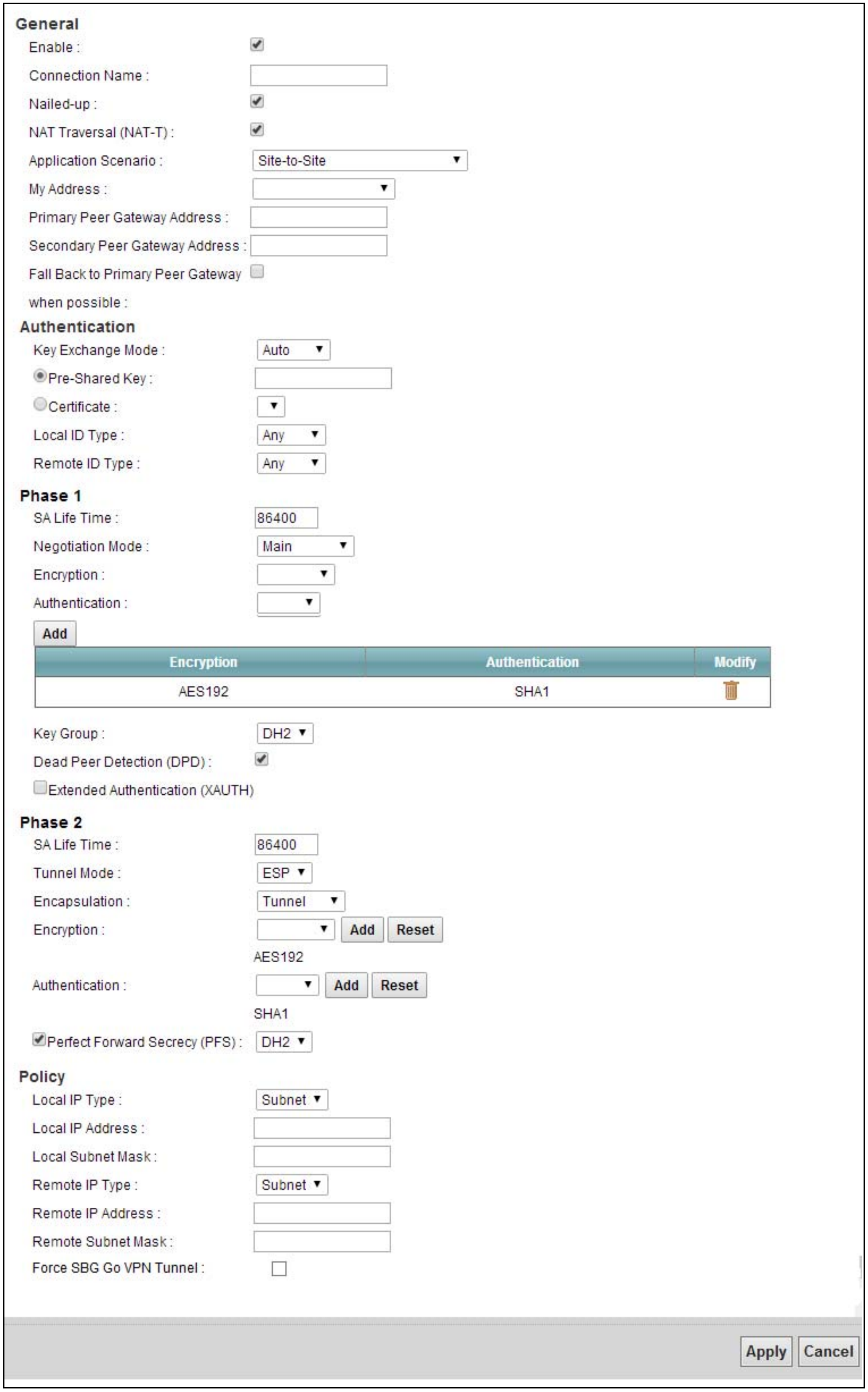
You can click the **Add New Entry** button or a policy's **Edit** icon in the **IPSec VPN > Setup** screen to either add or edit a VPN policy.

Note: The SBG3500-N uses the system default gateway interface's WAN IP address as its WAN IP address to set up a VPN tunnel.

20.4.2 The VPN Connection Add/Edit Screen

Configure the VPN connection settings in the **IPSec VPN > Setup > Edit** screen.

Figure 119 VPN > IPSec VPN > Setup > Edit



General

Enable : ☑

Connection Name :

Nailed-up : ☑

NAT Traversal (NAT-T) : ☑

Application Scenario : Site-to-Site ▼

My Address : ▼

Primary Peer Gateway Address :

Secondary Peer Gateway Address :

Fall Back to Primary Peer Gateway when possible : □

Authentication

Key Exchange Mode : Auto ▼

● Pre-Shared Key :

○ Certificate : ▼

Local ID Type : Any ▼

Remote ID Type : Any ▼

Phase 1

SA Life Time : 86400

Negotiation Mode : Main ▼

Encryption : ▼

Authentication : ▼

Add

Encryption	Authentication	Modify
AES192	SHA1	🗑

Key Group : DH2 ▼

Dead Peer Detection (DPD) : ☑

□ Extended Authentication (XAUTH)

Phase 2

SA Life Time : 86400

Tunnel Mode : ESP ▼

Encapsulation : Tunnel ▼

Encryption : ▼ Add Reset

AES192

Authentication : ▼ Add Reset

SHA1

☑ Perfect Forward Secrecy (PFS) : DH2 ▼

Policy

Local IP Type : Subnet ▼

Local IP Address :

Local Subnet Mask :

Remote IP Type : Subnet ▼

Remote IP Address :

Remote Subnet Mask :

Force SBG Go VPN Tunnel : □

Apply Cancel

The following table describes the labels in this screen.

Table 89 VPN > IPSec VPN > Setup > Edit

LABEL	DESCRIPTION
General	
Enable	Select the checkbox to activate this VPN policy.
Connection Name	Enter a name to identify this VPN policy. If you are editing an existing policy, this field is not editable. Note: The **Connection Name** of an IPsec rule must be unique and cannot be changed once it has been created.
Nailed-up	Select this if you want the SBG3500-N to automatically renegotiate the IPSec SA when the VPN connection is down. This feature is only applicable if you set the **Application Scenario** to **Site-to-Site**. When **Nailed-up** is enabled, you cannot disconnect the specified IPsec VPN tunnel in the **VPN** > **IPSec VPN** > **Monitor** screen.
NAT Traversal (NAT-T)	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router. Note: It is suggested to always enable the **NAT Traversal (NAT-T)** feature if you are not sure if a NAT device is connected to your VPN gateway. Once this feature is enabled, it will automatically detect connected NAT devices for you.
Application Scenario	Select the scenario that best describes your intended VPN connection. **Site-to-Site** - Choose this if the remote IPSec router has a static IP address or a domain name. This SBG3500-N can initiate the VPN tunnel. **Site-to-Site with Dynamic Peer** - Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. **Remote Access** - Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
My Address	Select an interface from the drop-down list and its IP address will be shown. The IP address of the SBG3500-N is the IP address of the interface. Note:
Primary Peer Gateway Address	Type a primary gateway address in this field. The primary peer gateway address is applicable (and required) when you choose **Site-to-Site** in the Application Scenario field. The SBG3500-N primarily attempts to establish the VPN tunnel with this remote address. The peer gateway address can be either an IP address or FQDN.
Secondary Peer Gateway Address	Type a secondary gateway address in this field. The secondary peer gateway IP address is applicable (and optional) if you choose **Site-to-Site** in the Application Scenario field. The SBG3500-N attempts to establish the VPN tunnel with this remote address if it fails to connect to the primary peer gateway address. The secondary peer gateway address can be either an IP address or FQDN.
Fall Back to Primary Peer Gateway when possible	When this box is checked, the SBG3500-N attempts to re-connect to the primary peer gateway address again when it is back up. The SBG3500-N will use secondary gateway address when the primary address is down. The VPN connection is briefly lost when SBG3500-N tries to reconnect using the primary address. Note that the peer devices using the secondary address cannot use a **nailed-up** VPN connecton setting.

Table 89 VPN > IPSec VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Authentication	Note: The SBG3500-N and remote IPSec router must use the same authentication method to establish the IKE SA.
Key Exchange Mode: Auto, Manual.	
Auto	
Pre-Shared Key	Select this to have the SBG3500-N and remote IPSec router use a pre-shared key (password) to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be • 8 - 32 alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • 8 - 32 pairs of hexadecimal (0-9, A-F) characters, preceded by “0x”. If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs. The SBG3500-N and remote IPSec router must use the same pre-shared key. Note: All remote access application scenario of IPsec rules must use the same pre-shared key.
Certificate	In order to use **Certificate** for IPsec authentication, you need to add new host certificates in the **Security** > **Certificates** screen. See a tutorial on how to add new host certificates in Chapter 4 on page 61. Select this to have the SBG3500-N and remote IPSec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the SBG3500-N uses to identify itself to the remote IPsec router. This certificate is one of the certificates in **Certificates**. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA. Note: The IPSec routers must trust each other’s certificates. The SBG3500-N uses one of its **Trusted Certificates** to authenticate the remote IPSec router’s certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router’s certificate.
Local/Remote ID Type	Select which type of identification is used to identify the SBG3500-N during authentication. **Any** - The SBG3500-N does not check the identity of the itself/remote IPSec router. **IP** - The SBG3500-N/remote IPSec router is identified by its IP address. **FQDN** - The SBG3500-N/remote IPSec router is identified by a domain name. **User-FQDN** - The SBG3500-N/remote IPSec router is identified by an e-mail address. Note: The options **FQDN** and **User-FQDN** of **Local ID Type** and **Remote ID Type** are not applicable if you select **Main** as the **Negotiation Mode** with **Pre-Shared Key**.
Manual	
SPI (HEX)	Type a hexadecimal value (between 256 and 4095) for the Security Parameter Index (SPI). Make sure the remote VPN endpoint has the same value in its SPI field.

Table 89 VPN > IPSec VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Tunnel Mode	Choose from the following tunnel modes in the drop-down list. • Encasulated Security Payload (**ESP**) - provides encrytption and the same services offered by AH, but its authentication is weaker. If you select ESP, you must select an Encryption algorithm and Authentication algorithm. • Authenticating Header (**AH**) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select AH, you must select an Authentication algorith. specifies the authentication protocol for the VPN header. Note the AH settings must match the remote VPN endpoint.
Encapsulation	Choose the encapsulation method for the VPN from the drop-down list. • **Tunnel** - encrypts the IP header information and the data. • **Transport** - encrypts the data. The SBG3500-N and remote IPSec router must use the same encapsulation.
Encryption	Choose the encryption algorithm for the ESP mode from the drop-down list. **DES** - a 56-bit key with the DES encryption algorithm, the default **3DES** - a 168-bit key with the DES encryption algorithm, more secure **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The SBG3500-N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Encryption Key (CHAR)	Type the encryption key (any alphanumeric characters or ,;|’~!@#$%^&*()_+\{}”:<>/=) in the field per following rule. **DES** - 8-31 characters **3DES** - 24-31 characters **AES128** - 16-32 characters **AES192** - 24-31 characters **AES256** - 31 characters You can also use hexadecimal by typing “0x” in the beginning of the key. The remote IPSec router must have the same encryption key.
Authentication	Choose the authentication algorithm from the drop-down list. • **MD5** - default • **SHA1** - more secure
Authentication Key	Tye the encryption key (any alphanumeric characters or ,;|’~!@#$%^&*()_+\{}”:<>/=) in the field per following rule. **MD5** - 16-20 characters **SHA1** - 20 characters You can also use hexadecimal by typing “0x” in the beginning of the key. The remote IPSec router must have the same encryption key.

Table 89 VPN > IPSec VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Phase 1	Phase 1 **Encryption** and **Authentication** can have up to 3 algorithm pairs. You cannot use phase 1 **Encryption**, **Authentication**, and **Key Group** pairs that already exist in other enabled IPsec rules with **Remote Access** selected as the **Application Scenario**. AES is considered as the same encryption regardless of bit length. The following are two examples: 1. Example1: An IPsec rule **remote1** has phase 1 **Encryption**, **Authentication**, and **Key Group** set as **3DES**, **SHA1**, and **DH2**. You cannot add new IPsec rule **remote2** to have the same algorithm pair. You can change either one algorithm to make it unique, such as using **3DES**, **SHA1**, and **DH1** for **remote2**. 2. IPsec rule **remote1** has phase1 **Encryption**, **Authentication**, and **Key Group** set as **AES256**, **SHA1**, and **DH2**. You cannot use **AES128**, **SHA1**, and **DH2** to add new IPsec rule **remote2** because AES is considered as the same regardless of bit length. Note: When the default IPsec rule **Default_L2TPVPN** is enabled, if you want to add a new **Remote Access IPsec** rule, you can use phase 1 **Encryption**, **Authentication**, and **Key Group** pair **DES**, **MD5**, and **DH2** or **DES**, **SHA1**, and **DH2**, or any algorithm combination with **DH1** or **DH5**.
SA Life Time	Define the length of time before an IKE or IPSec SA automatically renegotiates in this field. It may range from 1 to 99,999 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Negotiation Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are: **Main** - this encrypts the SBG3500-N’s and remote IPSec router’s identities but takes more time to establish the IKE SA. **Aggressive** - this is faster but does not encrypt the identities The SBG3500-N and the remote IPSec router must use the same negotiation mode.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The SBG3500-N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Add	Click this to add phase 1 **Encryption** and **Authentication**.
Modify	Select an entry and click the delete icon to remove it.

Table 89 VPN > IPSec VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Key Group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number **DH5** - use a 1536-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Dead Peer Detection (DPD)	Select this check box if you want the SBG3500-N to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the SBG3500-N sends a message to the remote IPSec router. If the remote IPSec router responds, the SBG3500-N transmits the data. If the remote IPSec router does not respond, the SBG3500-N shuts down the IKE SA.
Extended Authentication (XAUTH)	When multiple IPSec routers use the same VPN tunnel to connect to a single VPN tunnel (telecommuters sharing a tunnel for example), use extended authentication to enforce a user name and password check. This way even though they all know the VPN tunnel's security settings, each still has to provide a unique user name and password. Select the checkbox if one of the routers (the SBG3500-N or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server. Note: If you want to use Radius for **Extended Authentication (XAUTH)**, you need to configure the settings in the **VPN** > **IPSecVPN** > **Radius** screen beforehand. See Section 20.6 on page 267. Note: If you want to use **Local DB** for **Extended Authentication (XAUTH)**, make sure the user account exists in the **Maintenance** > **User Account** screen.
Phase 2	Phase 2 **Encryption** can have up to 3 different algorithms and **Authentication** can have up to 2 different algorithms. To add new algorithms, click the **Add** button next to **Encryption** or **Authentication**.
SA Life Time	Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The SBG3500-N automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Tunnel Mode	Select the security protocols used for an SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication** algorithm. **ESP** (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. If you select **ESP**, you must select an **Encryption** algorithm and Authentication algorithm. Both **AH** and **ESP** increase processing requirements and latency (delay). The SBG3500-N and remote IPSec router must use the same active protocol.
Encapsulation	Select which type of encapsulation the IPSec SA uses. Choices are: **Tunnel** - this mode encrypts the IP header information and the data. **Transport** - this mode only encrypts the data. If you set **Encapsulation** to **Transport**, Policy (Local and Remote) is not applicable. The SBG3500-N and remote IPSec router must use the same encapsulation.

Table 89 VPN > IPSec VPN > Setup > Edit (continued)

LABEL	DESCRIPTION
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The SBG3500-N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number **DH5** - enable PFS and use a 1536-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Policy	
Local IP Type	Select the IP type of the local device that is linked to the IPSec router. • **Subnet** - you will need to enter the network mask address • **Single -** only a single PC (no LAN) at the remote endpoint • **Range -** you will need to enter a starting IP address and a finishing IP address
Local IP Address	Type the IP address of the device linked to the local IPSec router. This must match the remote IP address configured on the remote IPSec device.
Local Subnet Mask	Type the subnet mask address of the device linked to the local IPSec router. This must match the remote IP address configure on the remote IPSec device.
Remote IP Type	Choose the remote IP type of the device linked to the remote IPSec router. • **Subnet** - you will need to enter the network mask address • **Single -** only a single PC (no LAN) at the remote endpoint • **Range -** you will need to enter a starting IP address and a finishing IP address
Remote IP Address	Type the IP address of the device linked to the remote IPSec router. This must match the local IP address configured on the remote IPSec device.
Remote Subnet Mask	Type the subnet mask address of a device linked to the remote IPSec router. This must match the local IP address configured on the remote IPSec device.
Force SBG Go VPN Tunnel	Click this checkbox to force data traffic to go through VPN tunnel when its destination IP address matches an entry in the IPSec VPN policy rule.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to restore your previous settings.

20.4.3 The Default_L2TPVPN IPSec VPN Rule

A default IPSec VPN rule (**Default_L2TP_VPN**) is predefined. It can be edited but cannot be removed. This rule is used for L2TP VPN exclusively and is disabled by default.

The following table lists the default settings for the **Default_L2TP_VPN** IPSec VPN.

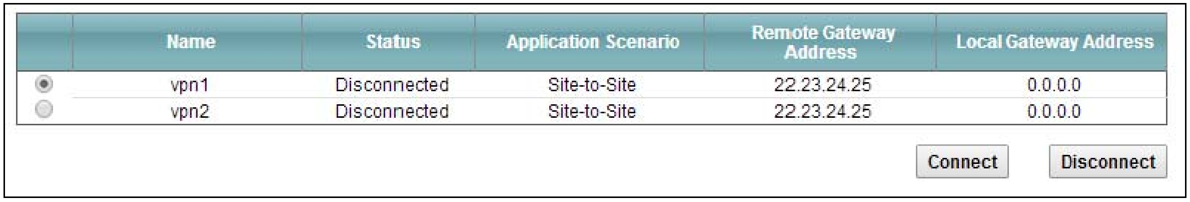
Table 90 Default settings for **Default_L2TP_VPN**

GENERAL		AUTHENTICATION	
Enabled	No	Pre-Shared Key	selected (text) 12345678
Nailed-up	No	Certificate	none
NAT Traversal	Yes	Local ID Type	IP
Application Scenario	Remote Access	Content	0.0.0.0
My Address	Any	Remote ID Type	Any
PHASE 1		**PHASE 2**	
Life time	86400	Life time	3600
Negotiation Mode	Main	Tunnel Mode	ESP
Encryption / Authentication	3DES / SHA1 3DES / MD5 AES256 / SHA1	Encryption	DES 3DES AES256
		Authentication	MD5 SHA1
Key Group	DH2	Perfect Forward Secrecy (PFS)	No
Dead Peer Detection (DPD)	Yes	Encapsulation	Transport
XAUTH	No		

20.5 The IPSec VPN Monitor Screen

In the Web Configurator, click **VPN > IPSec VPN > Monitor**. Use this screen to display and manage active VPN connections.

Figure 120 VPN > IPSec VPN > Monitor



	Name	Status	Application Scenario	Remote Gateway Address	Local Gateway Address
●	vpn1	Disconnected	Site-to-Site	22.23.24.25	0.0.0.0
○	vpn2	Disconnected	Site-to-Site	22.23.24.25	0.0.0.0

The following table describes the labels in this screen.

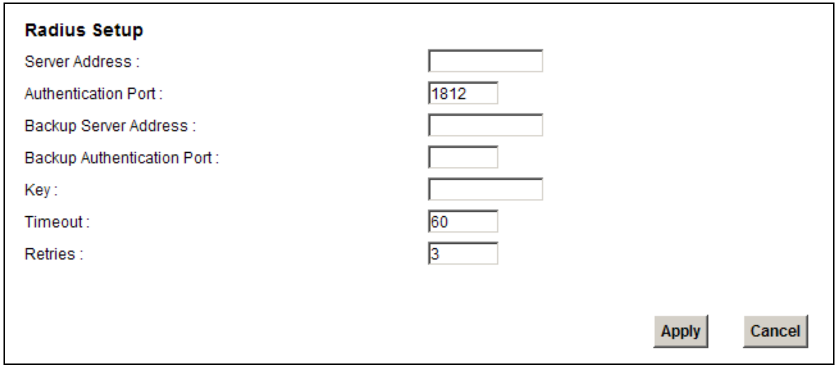
Table 91 VPN > IPSec VPN > Monitor

LABEL	DESCRIPTION
Radio Buttons	Click the radio button to choose the VPN client you want to connect or disconnect.
Name	This field displays the identification name for this IPSec VPN policy.
Status	This field displays whether the IPSec VPN connection is up (yellow bulb) or down (gray bulb).
Application Scenario	This field displays the encryption algorithm used for an SA.
Remote Gateway Address	This is the WAN IP address of the remote IPSec Gateway device.
Local Gateway Address	This is the WAN IP address of the local IPSec Gateway device.
Connect	Click this to connect.
Disconnect	Click this to disconnect.

20.6 The Radius Screen

Use the **Radius** screen to manage the list of RADIUS servers the SBG3500-N can use in authenticating users. In the Web Configurator, click **VPN > IPSec VPN > Radius**.

Figure 121 VPN > IPSec VPN > Radius



Radius Setup

Server Address :	
Authentication Port :	1812
Backup Server Address :	
Backup Authentication Port :	
Key :	
Timeout :	60
Retries :	3

The following table describes the labels in this screen.

Table 92 VPN > IPSec VPN > Radius

LABEL	DESCRIPTION
Radius Setup	
Server Address	Enter the address of the RADIUS server.
Authentication Port	Specify the port number on the RADIUS server to which the SBG3500-N sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup server, enter its address here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the SBG3500-N sends authentication requests. Enter a number between 1 and 65535.

Table 92 VPN > IPSec VPN > Radius (continued)

LABEL	DESCRIPTION
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the SBG3500-N. The key is not sent over the network. This key must be the same on the external authentication server and the SBG3500-N.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the SBG3500-N disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
Retries	Specify the number of connection retries before the SBG3500-N disconnects from the RADIUS server.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to restore your previous settings.

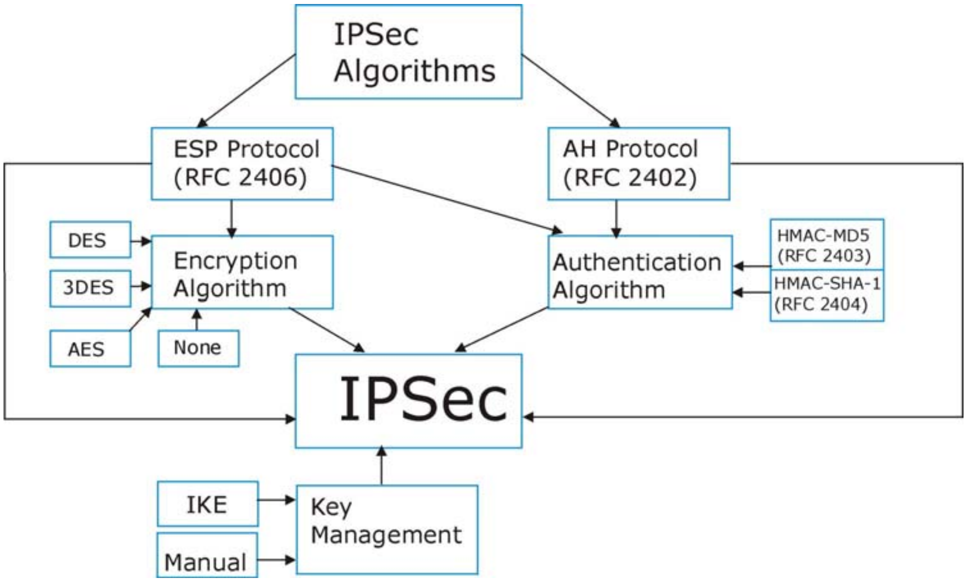
20.7 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

20.7.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 122 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

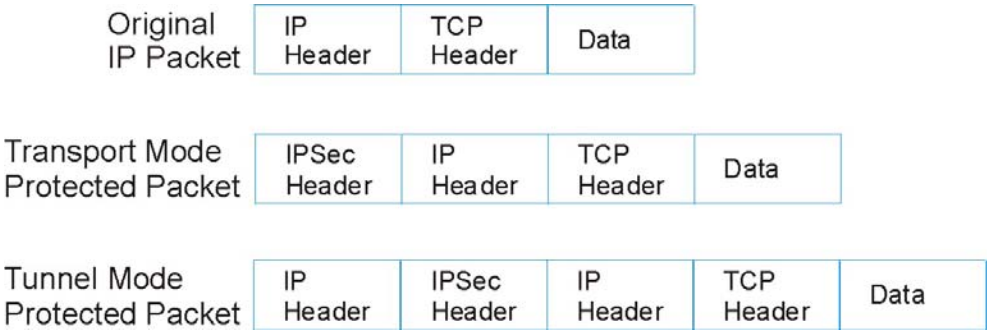
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

20.7.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the SBG3500-N supports **Tunnel** mode only.

Figure 123 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

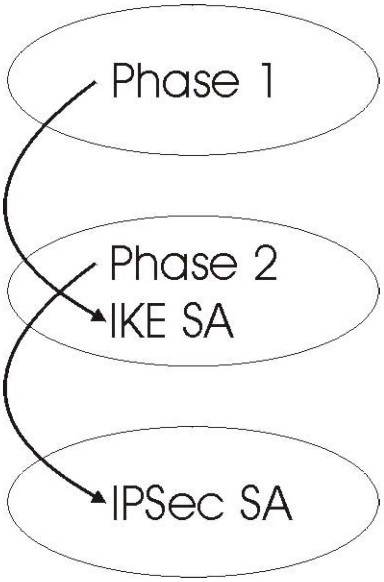
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

20.7.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 124 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The SBG3500-N automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

20.7.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

20.7.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the SBG3500-N.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 93 VPN and NAT

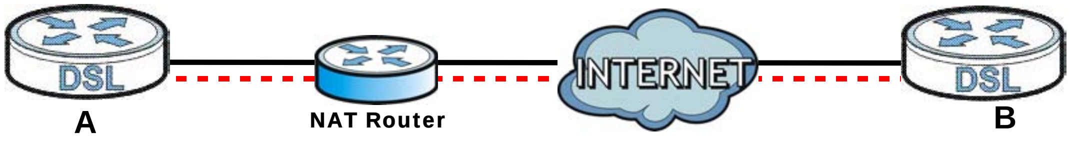
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

20.7.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the SBG3500-N's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 125 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 94 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N

Table 94 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the SBG3500-N if you enable NAT traversal.

20.7.7 ID Type and Content

With aggressive negotiation mode (see Section 20.7.4 on page 271), the SBG3500-N identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the SBG3500-N to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the SBG3500-N does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 20.7.4 on page 271), the ID type and content are encrypted to provide identity protection. In this case the SBG3500-N can only distinguish between different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The SBG3500-N can distinguish incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section 20.4 on page 257). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 95 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
FQDN	Type a domain name (up to 31 characters) by which to identify this SBG3500-N.
User-FQDN	Type an e-mail address (up to 31 characters) by which to identify this SBG3500-N.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

20.7.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two SBG3500-Ns in this example can complete negotiation and establish a VPN tunnel.

Table 96 Matching ID Type and Content Configuration Example

SBG3500-N A	SBG3500-N B
Local ID type: User-FQDN	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two SBG3500-Ns in this example cannot complete their negotiation because SBG3500-N B's **Local ID type** is **IP**, but SBG3500-N A's **Remote ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 97 Mismatching ID Type and Content Configuration Example

SBG3500-N A	SBG3500-N B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: User-FQDN	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

20.7.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 20.7.3 on page 270 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

20.7.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit, 1024-bit 1536-bit, 2048-bit, and 3072-bit Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

PPTP VPN

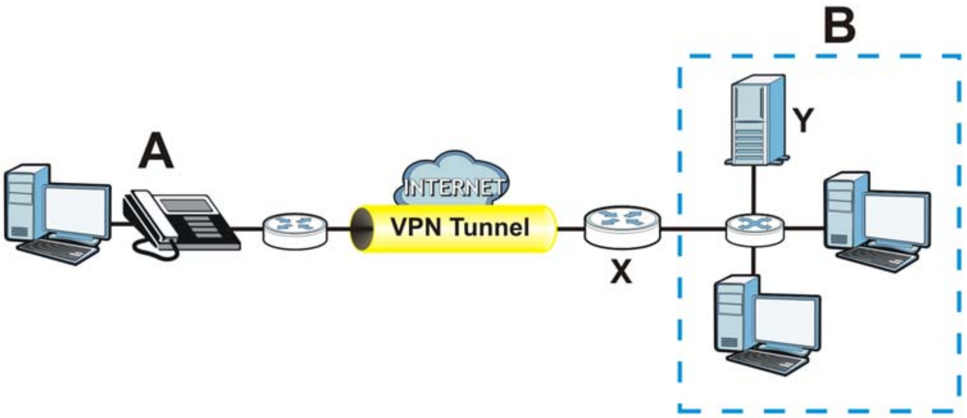
21.1 Overview

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a VPN using TCP/IP-based networks. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

PPTP sets up two sessions and uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers. It is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

PPTP works on a client-server model and is suitable for remote access applications. For example, an employee (**A**) can connect to the PPTP VPN gateway (**X**) as a PPTP client to gain access to the company network resources from outside the office. When you connect to a remote network (**B**) through a PPTP VPN, all of your traffic goes through the PPTP VPN gateway (**X**).

Figure 126 PPTP VPN Example



21.2 What You Can Do in this Chapter

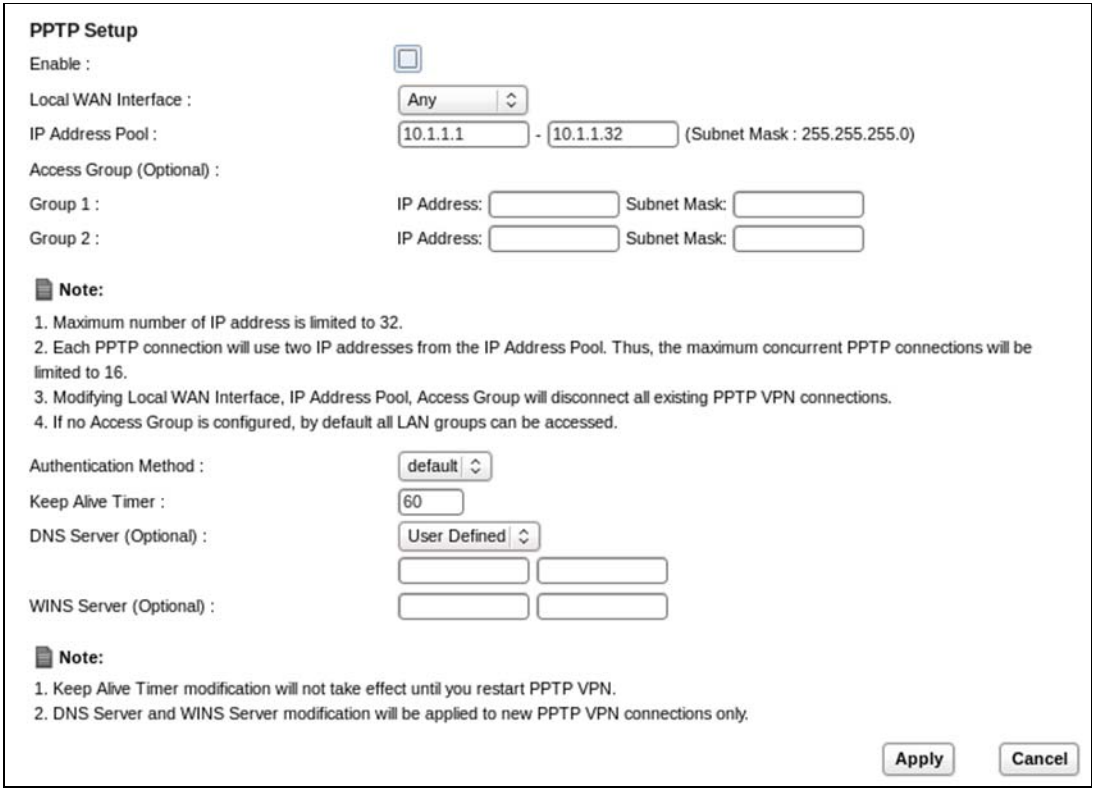
- Use the **Setup** screen to configure the PPTP VPN settings in the SBG3500-N (Section 21.3 on page 276).
- Use the **Monitor** screen to view settings for PPTP clients (Section 21.4 on page 277).

21.3 PPTP VPN Setup

Use this screen to configure settings for a Point to Point Tunneling Protocol (PPTP) server.

Click **VPN > PPTP VPN** to open the **Setup** screen as shown next.

Figure 127 VPN > PPTP VPN > Setup



PPTP Setup

Enable : □

Local WAN Interface : Any

IP Address Pool : 10.1.1.1 - 10.1.1.32 (Subnet Mask : 255.255.255.0)

Access Group (Optional) :

Group 1 : IP Address: Subnet Mask:

Group 2 : IP Address: Subnet Mask:

Note:

1. Maximum number of IP address is limited to 32.
2. Each PPTP connection will use two IP addresses from the IP Address Pool. Thus, the maximum concurrent PPTP connections will be limited to 16.
3. Modifying Local WAN Interface, IP Address Pool, Access Group will disconnect all existing PPTP VPN connections.
4. If no Access Group is configured, by default all LAN groups can be accessed.

Authentication Method : default

Keep Alive Timer : 60

DNS Server (Optional) : User Defined

WINS Server (Optional) :

Note:

1. Keep Alive Timer modification will not take effect until you restart PPTP VPN.
2. DNS Server and WINS Server modification will be applied to new PPTP VPN connections only.

This screen contains the following fields:

Table 98 VPN > PPTP VPN > Setup

LABEL	DESCRIPTION
PPTP Setup	
Enable	Use this field to turn the SBG3500-N'S PPTP VPN function on or off.
Local WAN Interface	Select an interface from the drop-down list and its IP address will be shown. This is the WAN interface upon which PPTP VPN listens to a client's connection request.
IP Address Pool	Enter the pool of IP addresses that the SBG3500-N uses to assign to the PPTP VPN clients. Note: This is with a 24-bit netmask and should not conflict with any configured WAN, LAN, DMZ, WLAN, or L2TP VPN subnet even if they are not in use.
Access Group (Optional)	Specify up to 2 LAN groups (subnets) which a PPTP VPN client is allowed to access. If none is specified, all LAN groups can be accessed. Enter the IP address and subnet mask for the LAN group(s).

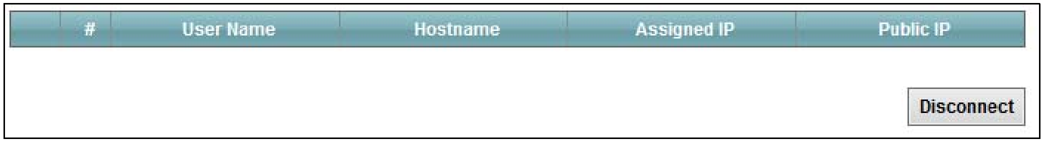
Table 98 VPN > PPTP VPN > Setup (continued)

LABEL	DESCRIPTION
Authentication Method	Select how the SBG3500-N authenticates a remote user before allowing access to the PPTP VPN tunnel. The authentication method has the SBG3500-N check a user's user name and password against the SBG3500-N's local database, which is configured in the **Maintenance** > **User Account** screen.
Keep Alive Timer	The SBG3500-N sends a Hello message after waiting this long without receiving any traffic from the remote user. The SBG3500-N disconnects the VPN tunnel if the remote user does not respond.
DNS Server (Optional)	Specify the IP addresses of DNS servers to assign to the remote users. You can choose from one of the DNS servers from the list, or choose User Defined to enter the static IP addresses for the first and second DNS servers manually.
WINS Server (Optional)	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to restore your previous settings.

21.4 The PPTP VPN Monitor Screen

In the Web Configurator, click **VPN > PPTP VPN > Monitor**. Use this screen to view settings for PPTP clients.

Figure 128 VPN > PPTP VPN > Monitor



The following table describes the labels in this screen.

Table 99 VPN > PPTP VPN > Monitor

LABEL	DESCRIPTION
User Name	This field displays the client's login name for this connection.
Hostname	This is the client's host name of this connection.
Assigned IP	This is the local point-to-point IP address assigned to the client.
Public IP	This is the client's public IP address for this connection.
Disconnect	Select a VPN client connection and click this to disconnect.

21.5 PPTP VPN Troubleshooting Tips

This section lists the common troubleshooting tips for PPTP VPN.

1 A PPTP client device (such as a PC, smart phone, tablet) cannot connect to the SBG3500-N.

TIP: This could be due to one of the following reasons:

a. The client device is not connected to the Internet successfully.

Action: Check the client device's Internet connection.

b. Incorrect server address configured on the client device.

(1) If the **Local WAN Interface** is **"Any"**:

From the SBG3500-N's GUI, click **Status**. The client device should be configured with one of the WAN interface IP addresses.

(2) If the **Local WAN Interface** is an interface (IP address shown to the right):

Use that IP address for the client device to connect.

c. The WAN interface which the SBG3500-N's PPTP VPN is using is not connected.

Action: From the SBG3500-N's GUI, click **Status**. Check if the WAN interface the client device is connected has an IP address present.

d. The PPTP VPN is not enabled.

Action: From the SBG3500-N's GUI, click **VPN** > **PPTP VPN**. Check **Enable** checkbox and click **Apply**.

e. PPTP is not configured correctly on the client device.

Action: Refer to Section 4.14 on page 69 for an example of PPTP VPN.

f. The client entered an incorrect username or password.

Action: From the SBG3500-N's GUI, click **Maintenance** > **User Account**. The client should use one of the accounts to make the connection.

g. The SBG3500-N has already reached the maximum number of concurrent PPTP VPN connections.

Action: There are too many clients connected. Wait a while and then retry.

2 A PPTP client is disconnected unexpectedly.

Tip: A PPTP connection will be dropped when one of the followings occurs on the SBG3500-N:

a. The client has no activity for a period of time.

b. The client loses connectivity to the SBG3500-N for a period of time.

c. PPTP VPN is disabled on the SBG3500-N.

d. When any one of these configuration changes is applied on the SBG3500-N: WAN interface used for PPTP VPN, IP address pool, access group.

e. The SBG3500-N's WAN interface on which the PPTP connection is established is disconnected.

3 A PPTP client is connected successfully but cannot access the local host or server behind the SBG3500-N.

Tip: This may be caused by one of the followings:

a. The local host or server is disconnected.

b. The access group is not configured correctly. From the SBG3500-N's GUI, go to **VPN** > **PPTP VPN** > **Setup** to check. Note that all local hosts are by default accessible unless access group is configured.

c. **IP Address Pool** for PPTP VPN conflicts with any WAN, LAN, DMZ, WLAN, or L2TP VPN subnet configured on the SBG3500-N. Note that the **IP Address Pool** for PPTP VPN has a 24-bit netmask and should not conflict with any others listed above even if they are not in use.

4 A PPTP client is connected successfully but cannot browse the Internet.

Tip: From the SBG3500-N's GUI, click **VPN** > **PPTP VPN** > **Setup**. Check if **DNS Server** is configured. A client cannot browse the Internet without DNS resolved. Note that when a new DNS server is configured, the client must disconnect then reconnect in order for the new DNS Server to take effect.

5 An Android device cannot connect to the SBG3500-N's PPTP VPN.

Tip: Devices running an Android OS older than version 4.1 have issues with PPTP/MPPE encryption. Avoid using devices that run an Android OS older than version 4.1 for PPTP VPN connection.

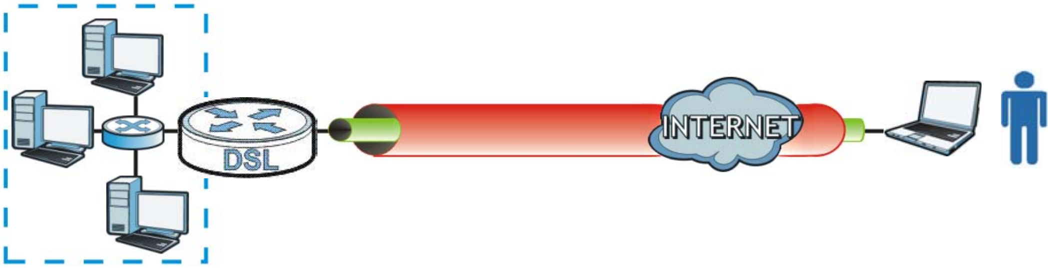
L2TP VPN

22.1 Overview

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel (defined by the IPSec VPN rule **Default_L2TPVPN**, refer to Section 20.4.3 on page 266) is established first and then an L2TP tunnel is built inside it. See Chapter 20 on page 256 for information on IPSec VPN.

L2TP VPN lets remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the SBG3500-N. The remote users do not need their own IPSec gateways or VPN client software.

Figure 129 L2TP VPN Overview



22.1.1 What You Can Do in this Chapter

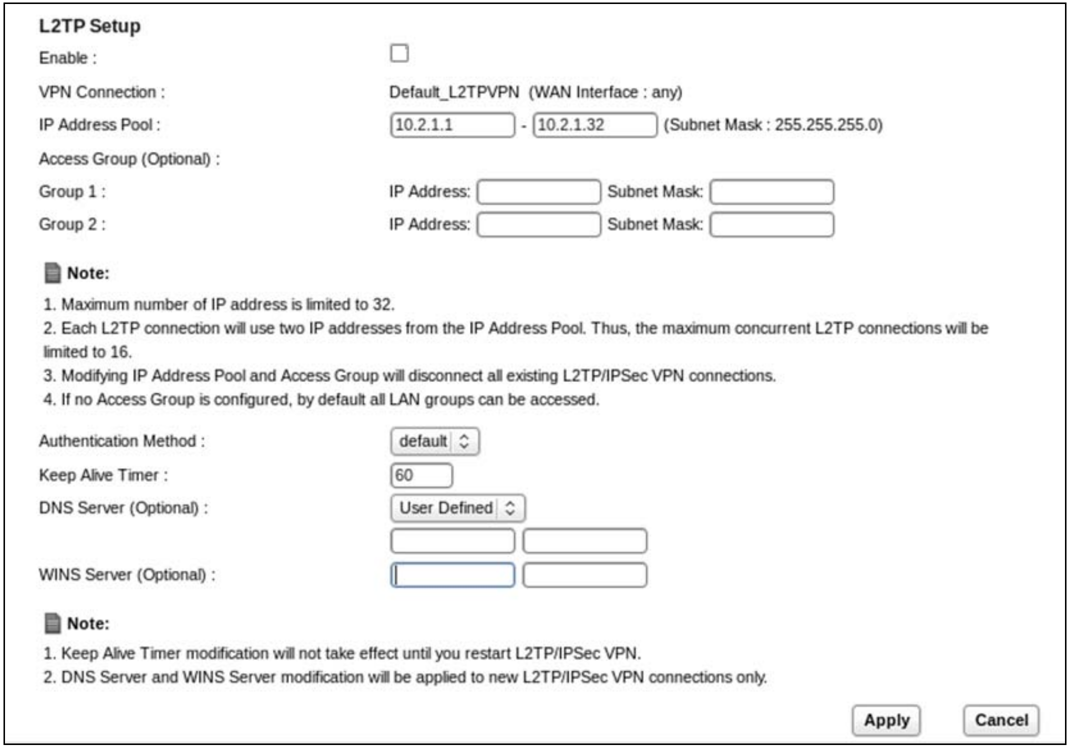
- Use the **L2TP VPN** screen to configure the SBG3500-N's L2TP VPN settings (Section 22.2 on page 281).
- Use the **Monitor** screen to view settings for L2TP clients (Chapter 22 on page 282).

Note: You need to configure the **Default_L2TPVPN** VPN rule in the **VPN** > **IPSec** > **IPSec Setup** screen. See Chapter 20 on page 256 for information on IPSec VPN.

22.2 L2TP VPN Screen

Click **VPN > L2TP VPN** to open the **Setup** screen. Use this screen to configure the SBG3500-N’s L2TP VPN settings.

Figure 130 VPN > L2TP VPN > Setup



L2TP Setup

Enable : □

VPN Connection : Default_L2TPVPN (WAN Interface : any)

IP Address Pool : 10.2.1.1 - 10.2.1.32 (Subnet Mask : 255.255.255.0)

Access Group (Optional) :

Group 1 : IP Address: Subnet Mask:

Group 2 : IP Address: Subnet Mask:

Note:

1. Maximum number of IP address is limited to 32.
2. Each L2TP connection will use two IP addresses from the IP Address Pool. Thus, the maximum concurrent L2TP connections will be limited to 16.
3. Modifying IP Address Pool and Access Group will disconnect all existing L2TP/IPSec VPN connections.
4. If no Access Group is configured, by default all LAN groups can be accessed.

Authentication Method : default

Keep Alive Timer : 60

DNS Server (Optional) : User Defined

WINS Server (Optional) :

Note:

1. Keep Alive Timer modification will not take effect until you restart L2TP/IPSec VPN.
2. DNS Server and WINS Server modification will be applied to new L2TP/IPSec VPN connections only.

The following table describes the fields in this screen.

Table 100 VPN > L2TP VPN > Setup

LABEL	DESCRIPTION
Enable	Select the checkbox to enable the SBG3500-N’s L2TP VPN function.
VPN Connection	This is the WAN interface where L2TP VPN listens for a client connection request. It is configured in the **Default_L2TPVPN** IPSec VPN rule in the **VPN** > **IPSec** > **IPSec Setup** screen. See Chapter 20 on page 256 for information on IPSec VPN.
IP Address Pool	Enter the pool of IP addresses that the SBG3500-N uses to assign to the L2TP VPN clients. Note: These addresses use a 24-bit netmask and should not conflict with any WAN, LAN, DMZ, WLAN, or PPTP VPN subnet even if they are not in use.
Access Group (Optional)	Specify up to 2 LAN groups (subnets) which a L2TP VPN client is allowed to access. If none is specified, all LAN groups can be accessed. Enter the IP address and subnet mask for the LAN group(s).
Authentication Method	Select how the SBG3500-N authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the SBG3500-N check a user’s user name and password against the SBG3500-N’s local database, which is configured in the **Maintenance** > **User Account** screen.

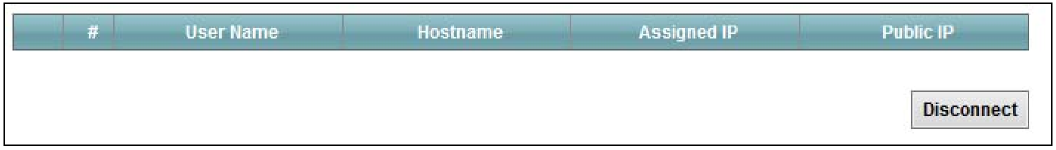
Table 100 VPN > L2TP VPN > Setup (continued)

LABEL	DESCRIPTION
Keep Alive Timer	The SBG3500-N sends a Hello message after waiting this long without receiving any traffic from the remote user. The SBG3500-N disconnects the VPN tunnel if the remote user does not respond.
DNS Server (Optional)	Specify the IP addresses of DNS servers to assign to the remote users. You can choose from one of the DNS servers from the list, or choose User Defined to enter the static IP addresses for the first and second DNS servers manually.
WINS Server (Optional)	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to restore your previous settings.

22.3 The L2TP VPN Monitor Screen

In the Web Configurator, click **VPN > L2TP VPN > Monitor**. Use this screen to view settings for PPTP clients.

Figure 131 VPN > L2TP VPN > Monitor



	#	User Name	Hostname	Assigned IP	Public IP

The following table describes the labels in this screen.

Table 101 VPN > L2TP VPN > Monitor

LABEL	DESCRIPTION
User Name	This field displays the client's login name for this connection.
Hostname	This is the client's host name of this connection.
Assigned IP	This is the local point-to-point IP address assigned to the client.
Public IP	This is the client’s public IP address for this connection.
Disconnect	Select a VPN client connection and click this to disconnect.

22.4 L2TP VPN Troubleshooting Tips

This section lists the common troubleshooting tips for L2TP VPN.

1 A L2TP client device (such as a PC, smart phone, tablet) cannot connect to the SBG3500-N.

TIP: This could be due to one of the following reasons:

a. The client device is not connected to the Internet successfully.

Action: Check the client device’s Internet connection.

b. Incorrect server address configured on the client device.

Action: From the SBG3500-N’s GUI, click **VPN** > **IPSec VPN** > **Setup**.

(1) If the **Local Gateway Address** for **Default_L2TPVPN** is set to **“Any”**:

From the SBG3500-N’s GUI, click **Status**. The client device should be configured with one of the WAN interface IP addresses.

(2) If the **Local Gateway Address** for **Default_L2TPVPN** is an IP address:

Use that IP address for the client device to connect.

c. The WAN interface which the SBG3500-N’s L2TP VPN is using is not connected.

Action: From the SBG3500-N’s GUI, click **Status**. Check if the WAN interface used by L2TP VPN is connected.

d. The client device has an incorrect IPSec pre-shared key configured.

Action: From the SBG3500-N’s GUI, click **VPN** > **IPSec VPN** > **Edit Default_L2TPVPN**. The client device should use the same pre-shared key.

e. The L2TP VPN is not fully enabled.

Action: From the SBG3500-N’s GUI,

(1) Click **VPN** > **IPSec** > **Edit Default_L2TPVPN**. Select the **Enable** checkbox and click **Apply**.

(2) Click **VPN** > **L2TP VPN** > **Setup**. Select the **Enable** checkbox and click **Apply**.

f. L2TP or IPSec is not configured correctly on the client device.

Action: Refer to Section 4.15 on page 81 for an example of L2TP VPN.

g. The client entered an incorrect username or password.

Action: From the SBG3500-N’s GUI, click **Maintenance** > **User Account**. The client should use one of the accounts to make the connection.

h. The SBG3500-N exceeds the maximum number of concurrent L2TP VPN connections.

Action: There are too many clients connected. Wait a while and then retry.

2 A windows L2TP client fails to connect to the SBG3500-N with an "invalid certificate" message.

Tip: Windows sometimes may show this error even if the client device has been configured with a correct pre-shared key for authentication. This usually happens at the first connection attempt after a new connection profile is created. Reconfigure the pre-shared key on the client Windows device and retry the connection.

3 An L2TP client device cannot reconnect after it is disconnected.

Tip: If a client reconnects right after it is disconnected, the reconnection may fail. Wait 60 seconds before reconnecting.

4 An L2TP client is disconnected unexpectedly.

Tip: An L2TP connection will be dropped when one of the followings occurs on the SBG3500-N:

(1) Client has no activity for a period of time.

(2) Client loses connectivity to the SBG3500-N for a period of time.

(3) Any IPSec VPN configuration change is applied on the SBG3500-N.

(4) Either Default_L2TPVPN IPSec configuration or L2TP VPN is disabled on the SBG3500-N.

(5) When any one of these configuration changes is applied on the SBG3500-N: WAN Interface used for L2TP VPN, IP Address Pool, Access Group.

(6) The SBG3500-N WAN interface on which the L2TP connection established is disconnected.

5 An L2TP client is connected successfully but cannot access the local host or server behind the SBG3500-N.

Tip: This may be caused by one of the followings:

(1) The local host or server is disconnected.

(2) The Access Group is not configured correctly. From the SBG3500-N's GUI, go to the **VPN** > **L2TP VPN** > **Setup** screen to check. Note that all local hosts are by default accessible unless Access Group is configured.

(3) **IP Address Pool** for L2TP VPN is conflicting with any WAN, LAN, DMZ, WLAN, or PPTP VPN subnet configured on the SBG3500-N. Note that **IP Address Pool** for L2TP VPN has 24-bit netmask and should not conflict with any others listed above even if they are not in use.

6 An L2TP client is connected successfully but cannot browse Internet.

Tip: From the SBG3500-N's GUI, click **VPN** > **L2TP VPN** > **Setup**. Check if DNS Server is configured. A client cannot browse Internet without DNS resolved. Note that when a new DNS Server is configured, the client must disconnect then reconnect in order for the new DNS Server to take effect.

7 The L2TP client can no longer connect to SBG3500-N after the **Encryption** or **Authentication** for the **Default_L2TPVPN** IPSec VPN rule is changed.

Tip: A user usually do not need change the default **Encryption** or **Authentication** algorithms in the **Default_L2TPVPN** IPSec VPN rule. The default **Encryption** and **Authentication** algorithms should support the built-in L2TP/IPSec client software in the popular operating systems (Windows (XP, Vista, 7), Android, and iOS).

Refer to Table 90 on page 266 for the default setting of the **Default_L2TPVPN** IPSec VPN rule.

As a reference, Table 102 on page 285 lists the IPSec proposals provided by a built-in L2TP client in the popular operating systems during IPSec phase 1 negotiation. The first proposal that can be supported by the phase 1 setting in the **Default_L2TPVPN** IPSec VPN rule will be accepted by the

SBG3500-N. The algorithms in red in Table 102 on page 285 indicate the ones that will be accepted based on Table 90 on page 266.

Table 102 Phase 1 IPSec proposals provided by the built-in L2TP client in popular operating systems (Encryption/Authentication/Key Group)

	WINDOWS XP	WINDOWS VISTA	WINDOWS 7	IOS 5.1	ANDROID 4.1
1	3DES/SHA1/ DH15	3DES/SHA1/ DH15	AES/SHA1/DH15	AES/SHA1/DH2	AES/SHA1/DH2
2	3DES/SHA1/DH2	3DES/SHA1/DH2	3DES/SHA1/ DH15	AES/MD5/DH2	AES/MD5/DH2
3	3DES/MD5/DH2		3DES/SHA1/DH2	3DES/SHA1/DH2	3DES/SHA1/DH2
4	DES/SHA1/DH1			3DES/MD5/DH2	3DES/MD5/DH2
5	DES/MD5/DH1				DES/SHA1/DH2
6					DES/MD5/DH2

After phase 1 tunnel is established, IPSec phase 2 negotiations begin. Table 103 on page 285 lists the IPSec phase 2 proposals provided by a built-in L2TP client in the popular operating systems. The first proposal that can be supported by the phase 2 setting in the **Default_L2TPVPN** IPSec VPN rule will be accepted by the SBG3500-N. The algorithms in red in Table 103 on page 285 indicate the ones that will be accepted based on Table 90 on page 266.

Table 103 Phase 2 IPSec proposals provided by the built-in L2TP client in popular operating systems (Tunnel Mode/Encryption/Authentication) [Encapsulation = Transport]

	WINDOWS XP	WINDOWS VISTA	WINDOWS 7	IOS 5.1	ANDROID 4.1
1	ESP/3DES/MD5 ESP/3DES/SHA1	ESP/AES/SHA1	ESP/AES/SHA1	ESP/AES/SHA1 ESP/AES/MD5 ESP/3DES/SHA1 ESP/3DES/MD5	ESP/AES/SHA1 ESP/AES/MD5 ESP/3DES/SHA1 ESP/3DES/MD5 ESP/DES/SHA1 ESP/DES/MD5
2	AH/-/SHA1 and ESP/3DES/-	ESP/3DES/SHA1	ESP/3DES/SHA1		
3	AH/-/MD5 and ESP/3DES/-	AH/-/SHA1 and ESP/AES/-	ESP/DES/SHA1		
4	AH/-/SHA1 and ESP/3DES/SHA1	AH/-/SHA1 and ESP/3DES/-	ESP/-/SHA1		
5	AH/-/MD5 and ESP/3DES/MD5	AH/-/SHA1 and ESP/3DES/SHA1	AH/-/SHA1		
6	ESP/DES/MD5 ESP/DES/SHA1	ESP/-/SHA1			
		AH/-/SHA1			

23

Log

23.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Device log and then display the logs or have the Device send them to an administrator (as e-mail) or to a syslog server.

23.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 23.2 on page 287).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 23.3 on page 288).

23.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 104 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.

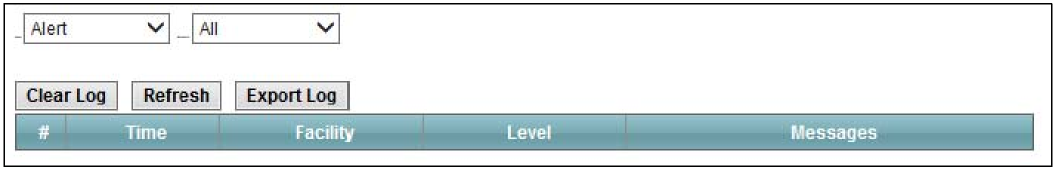
Table 104 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

23.2 The System Log Screen

Use the **System Log** screen to see the system logs. Click **System Monitor > Log** to open the **System Log** screen.

Figure 132 System Monitor > Log > System Log



The following table describes the fields in this screen.

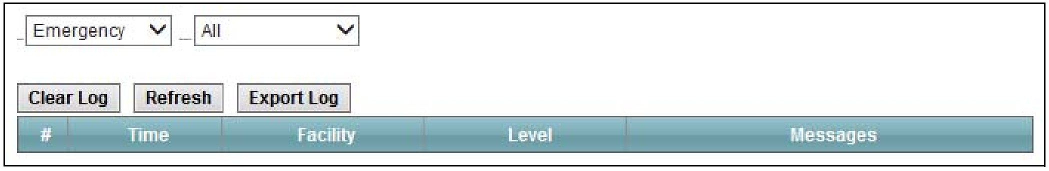
Table 105 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
System Log	
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

23.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 133 System Monitor > Log > Security Log



The following table describes the fields in this screen.

Table 106 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Logs Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

24

Network Status

24.1 Overview

Use the **Network Status** screens to look at network Network Status and statistics of the WAN and LAN interfaces.

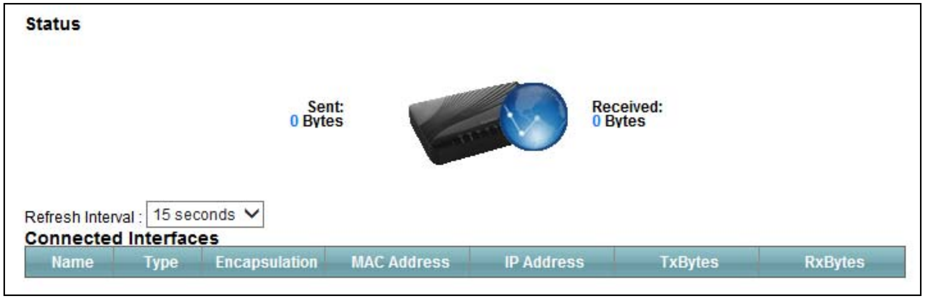
24.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 24.2 on page 289).
- Use the **LAN** screen to view the LAN traffic statistics (Section 24.3 on page 290).
- Use the **DHCP Client** screen to view the DHCP Client list (Section 24.4 on page 290).

24.2 The WAN Status Screen

Click **System Monitor > Network Status** to open the **WAN** screen. The figure in this screen shows the number of bytes received and sent on the SBG3500-N.

Figure 134 System Monitor > Network Status > WAN



The following table describes the fields in this screen.

Table 107 System Monitor > Network Status > WAN

LABEL	DESCRIPTION
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.

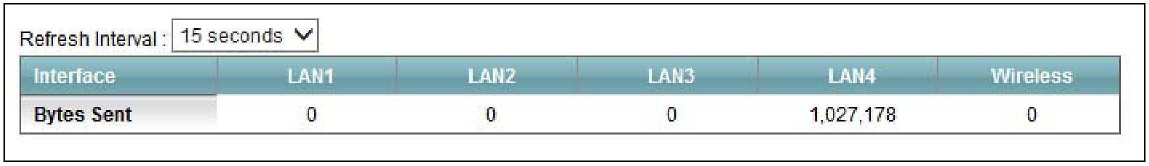
Table 107 System Monitor > Network Status > WAN (continued)

LABEL	DESCRIPTION
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

24.3 The LAN Status Screen

Click **System Monitor > Network Status > LAN** to open the following screen. The figure in this screen shows the interface that is currently connected on the SBG3500-N.

Figure 135 System Monitor > Network Status > LAN



Refresh Interval : 15 seconds

Interface	LAN1	LAN2	LAN3	LAN4	Wireless
Bytes Sent	0	0	0	1,027,178	0

The following table describes the fields in this screen.

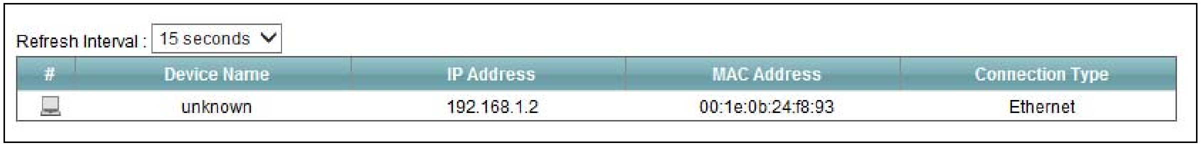
Table 108 System Monitor > Network Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the SBG3500-N to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.

24.4 The DHCP Client Screen

Click **System Monitor > Network Status > DHCP Client** to open the following screen. The figure in this screen shows the number of client devices that are connected to the SBG3500

System Monitor > Network Status > DHCP Client



Refresh Interval : 15 seconds

#	Device Name	IP Address	MAC Address	Connection Type
🖥	unknown	192.168.1.2	00:1e:0b:24:f8:93	Ethernet

The following table describes the fields in this screen.

Table 109 System Monitor > Network Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Choose the screen refresh time (15, 30, 60 seconds) from the drop-down list to see changes in the devices that are on the network.
#	This displays the device that is connected to the SBG3500-N.
Device Name	This displays the system name of the device on the SBG3500-N.

Table 109 System Monitor > Network Status > LAN

LABEL	DESCRIPTION
IP Address	This displays the IP address of the device on the SBG3500-N.
MAC Address	This displays the MAC address of the device on the SBG3500-N.
Connection Type	This displays the connection type that the device is using to connect to the SBG3500-N.

ARP Table

25.1 Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

25.1.1 How ARP Works

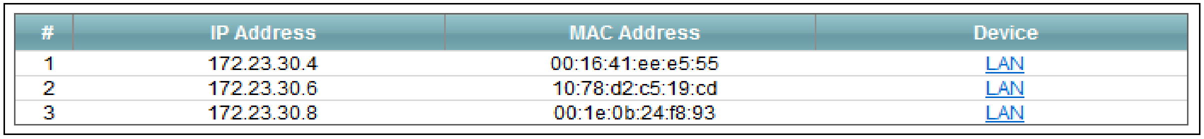
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

25.2 ARP Table Screen

Use the ARP table to view IP-to-MAC address mapping(s). To open this screen, click **System Monitor** > **ARP Table**.

Figure 136 System Monitor > ARP Table



#	IP Address	MAC Address	Device
1	172.23.30.4	00:16:41:ee:e5:55	LAN
2	172.23.30.6	10:78:d2:c5:19:cd	LAN
3	172.23.30.8	00:1e:0b:24:f8:93	LAN

The following table describes the labels in this screen.

Table 110 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a port.

Table 110 System Monitor > ARP Table (continued)

LABEL	DESCRIPTION
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click on the device type to go to its configuration screen.

26

Routing Table

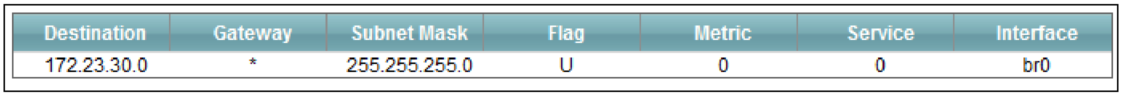
26.1 Overview

Routing is based on the destination address only and the Device takes the shortest path to forward a packet.

26.2 The Routing Table Screen

Click **System Monitor** > **Routing Table** to open the following screen.

Figure 137 System Monitor > Routing Table



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.23.30.0	*	255.255.255.0	U	0	0	br0

The following table describes the labels in this screen.

Table 111 System Monitor > Routing Table

LABEL	DESCRIPTION
Destination	This indicates the destination IP address of this route.
Gateway	This indicates the IP address of the gateway that helps forward this route’s traffic.
Subnet Mask	This indicates the destination subnet mask of this route.
Flag	This indicates the route status. **U-Up:** The route is up. **!-Reject:** The route is blocked and will force a route lookup to fail. **G-Gateway:** The route uses a gateway to forward traffic. **H-Host:** The target of the route is a host. **R-Reinstate:** The route is reinstated for dynamic routing. **D-Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect. **M-Modified (redirect):** The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".

Table 111 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Service	This indicates the name of the service used to forward the route.
Interface	This indicates the name of the interface through which the route is forwarded. **br0** indicates the LAN interface. **ptm0** indicates the WAN interface using IPoE or in bridge mode. **ppp0** indicates the WAN interface using PPPoE.

27

IGMP Status

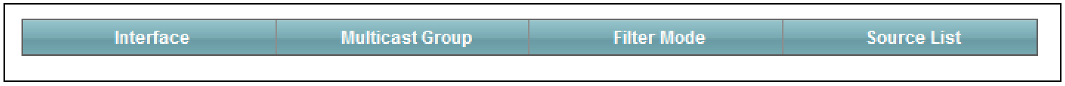
27.1 Overview

Use the **IGMP Status** screens to look at IGMP group status and traffic statistics.

27.2 The IGMP Group Status Screen

Use this screen to look at the current list of multicast groups the Device has joined and which ports have joined it. To open this screen, click **System Monitor > IGMP Group Status**.

Figure 138 System Monitor > IGMP Group Status



Interface	Multicast Group	Filter Mode	Source List

The following table describes the labels in this screen.

Table 112 System Monitor > IGMP Group Status

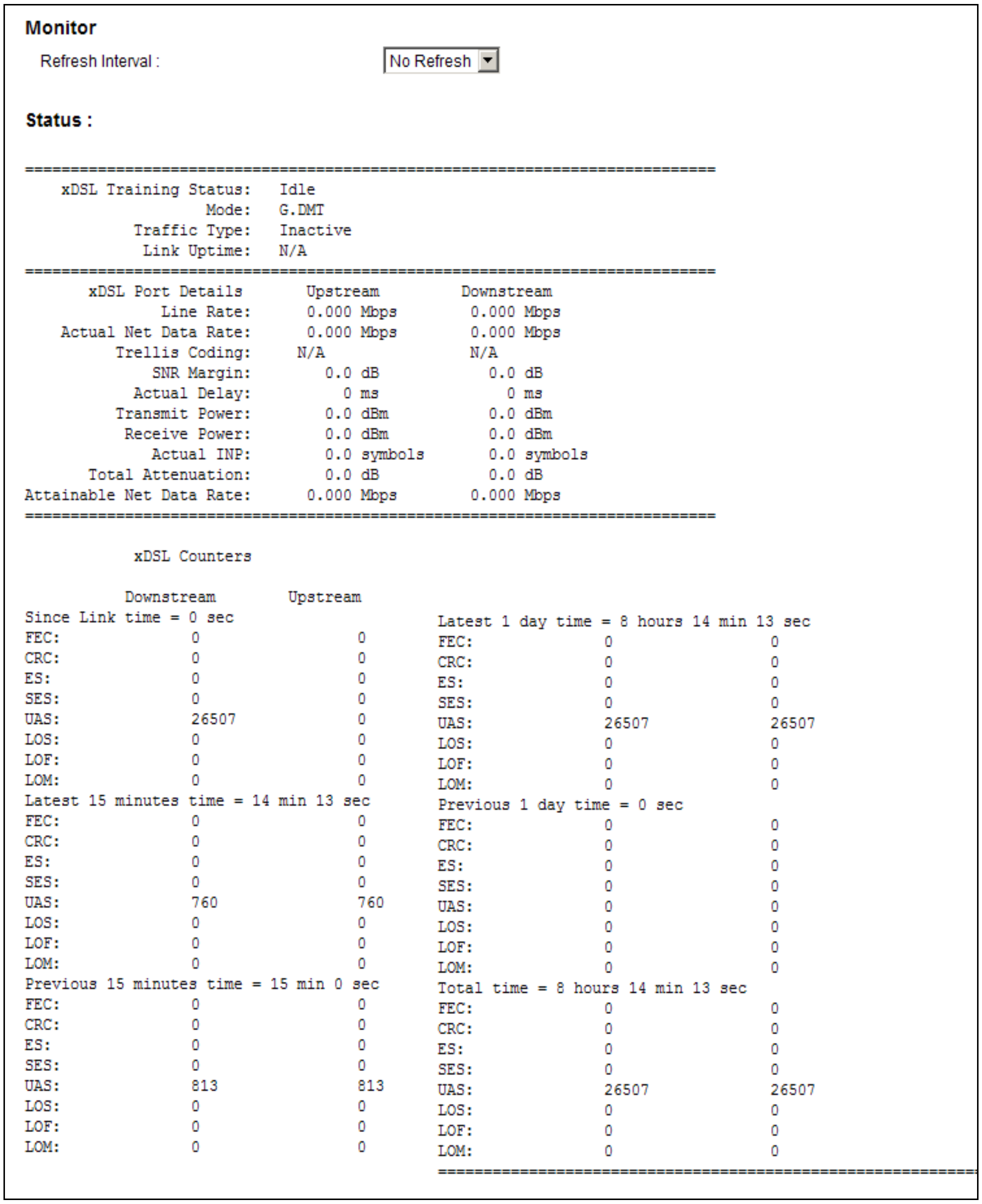
LABEL	DESCRIPTION
Interface	This field displays the name of an interface on the Device that belongs to an IGMP multicast group.
Multicast Group	This field displays the name of the IGMP multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group’s traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group’s traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group’s traffic depending on the filter mode.

xDSL Statistics

28.1 The xDSL Statistics Screen

Use this screen to view detailed DSL statistics. Click **System Monitor > xDSL Statistics** to open the following screen.

Figure 139 System Monitor > xDSL Statistics



Monitor

Refresh Interval : No Refresh

Status :

```
============================================================================
    xDSL Training Status:   Idle
                    Mode:   G.DMT
            Traffic Type:   Inactive
             Link Uptime:   N/A
============================================================================
       xDSL Port Details       Upstream         Downstream
               Line Rate:      0.000 Mbps       0.000 Mbps
    Actual Net Data Rate:      0.000 Mbps       0.000 Mbps
          Trellis Coding:     N/A              N/A
              SNR Margin:        0.0 dB           0.0 dB
            Actual Delay:          0 ms             0 ms
          Transmit Power:        0.0 dBm          0.0 dBm
           Receive Power:        0.0 dBm          0.0 dBm
              Actual INP:        0.0 symbols      0.0 symbols
       Total Attenuation:        0.0 dB           0.0 dB
Attainable Net Data Rate:      0.000 Mbps       0.000 Mbps
============================================================================

            xDSL Counters

           Downstream        Upstream
Since Link time = 0 sec                      Latest 1 day time = 8 hours 14 min 13 sec
FEC:              0                 0        FEC:              0                  0
CRC:              0                 0        CRC:              0                  0
ES:               0                 0        ES:               0                  0
SES:              0                 0        SES:              0                  0
UAS:              26507             0        UAS:              26507              26507
LOS:              0                 0        LOS:              0                  0
LOF:              0                 0        LOF:              0                  0
LOM:              0                 0        LOM:              0                  0
Latest 15 minutes time = 14 min 13 sec       Previous 1 day time = 0 sec
FEC:              0                 0        FEC:              0                  0
CRC:              0                 0        CRC:              0                  0
ES:               0                 0        ES:               0                  0
SES:              0                 0        SES:              0                  0
UAS:              760               760      UAS:              0                  0
LOS:              0                 0        LOS:              0                  0
LOF:              0                 0        LOF:              0                  0
LOM:              0                 0        LOM:              0                  0
Previous 15 minutes time = 15 min 0 sec      Total time = 8 hours 14 min 13 sec
FEC:              0                 0        FEC:              0                  0
CRC:              0                 0        CRC:              0                  0
ES:               0                 0        ES:               0                  0
SES:              0                 0        SES:              0                  0
UAS:              813               813      UAS:              26507              26507
LOS:              0                 0        LOS:              0                  0
LOF:              0                 0        LOF:              0                  0
LOM:              0                 0        LOM:              0                  0
                                             ===========================================================
```

The following table describes the labels in this screen.

Table 113 System Monitor > xDSL Statistics

LABEL	DESCRIPTION
Refresh Interval	Select the time interval for refreshing statistics.
xDSL Training Status	This displays the current state of setting up the DSL connection.
Mode	This displays the ITU standard used for this connection.
Traffic Type	This displays the type of traffic the DSL port is sending and receiving. **Inactive** displays if the DSL port is not currently sending or receiving traffic.
Link Uptime	This displays how long the port has been running (or connected) since the last time it was started.
xDSL Port Details	
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Line Rate	These are the data transfer rates at which the port is sending and receiving data.
Actual Net Data Rate	These are the rates at which the port is sending and receiving the payload data without transport layer protocol headers and traffic.
Trellis Coding	This displays whether or not the port is using Trellis coding for traffic it is sending and receiving. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable.
SNR Margin	This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets.
Actual Delay	This is the upstream and downstream interleave delay. It is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.
Transmit Power	This is the upstream and downstream far end actual aggregate transmit power (in dBm). Upstream is how much power the port is using to transmit to the service provider. Downstream is how much port the service provider is using to transmit to the port.
Receive Power	Upstream is how much power the service provider is receiving from the port. Downstream is how much power the port is receiving from the service provider.
Actual INP	Sudden spikes in the line's level of external noise (impulse noise) can cause errors and result in lost packets. This could especially impact the quality of multimedia traffic such as voice or video. Impulse noise protection (INP) provides a buffer to allow for correction of errors caused by error correction to deal with this. The number of DMT (Discrete Multi-Tone) symbols shows the level of impulse noise protection for the upstream and downstream traffic. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data.
Total Attenuation	This is the upstream and downstream line attenuation, measured in decibels (dB). This attenuation is the difference between the power transmitted at the near-end and the power received at the far-end. Attenuation is affected by the channel characteristics (wire gauge, quality, condition and length of the physical line).
Attainable Net Data Rate	These are the highest theoretically possible transfer rates at which the port could send and receive payload data without transport layer protocol headers and traffic.
xDSL Counters	

Table 113 System Monitor > xDSL Statistics (continued)

LABEL	DESCRIPTION
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
FEC	This is the number of Far End Corrected blocks.
CRC	This is the number of Cyclic Redundancy Checks.
ES	This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect.
SES	This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES.
UAS	This is the number of UnAvailable Seconds.
LOS	This is the number of Loss Of Signal seconds.
LOF	This is the number of Loss Of Frame seconds.
LOM	This is the number of Loss of Margin seconds.

29

User Account

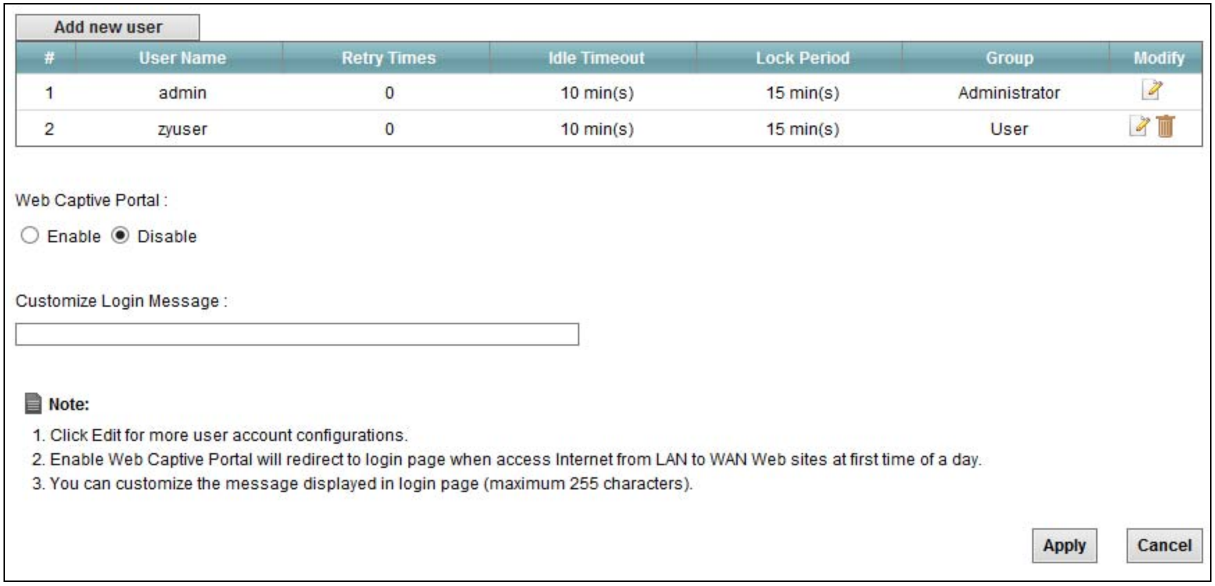
29.1 Overview

Use the **User Account** screen to manage user accounts, which includes configuring the username, password, retry times, file sharing, captive portal, and customizing the login message.

29.2 The User Account Screen

Click **Maintenance > User Account** to open the following screen.

Figure 140 Maintenance > User Account



#	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	admin	0	10 min(s)	15 min(s)	Administrator	✎
2	zyuser	0	10 min(s)	15 min(s)	User	✎ 🗑

Web Captive Portal :

○ Enable ● Disable

Customize Login Message :

Note:

1. Click Edit for more user account configurations.
2. Enable Web Captive Portal will redirect to login page when access Internet from LAN to WAN Web sites at first time of a day.
3. You can customize the message displayed in login page (maximum 255 characters).

The following table describes the labels in this screen.

Table 114 Maintenance > User Account

LABEL	DESCRIPTION
Add new user	Click this to configure a new user account.
#	This is the index number of the entry.
User Name	This field displays the name of the user.
Retry Times	This field indicates how many times a user can re-enter his/her account information before the Device locks the user out.
Idle Timeout	This field indicates the number of minutes that the system can idle before being logged out.

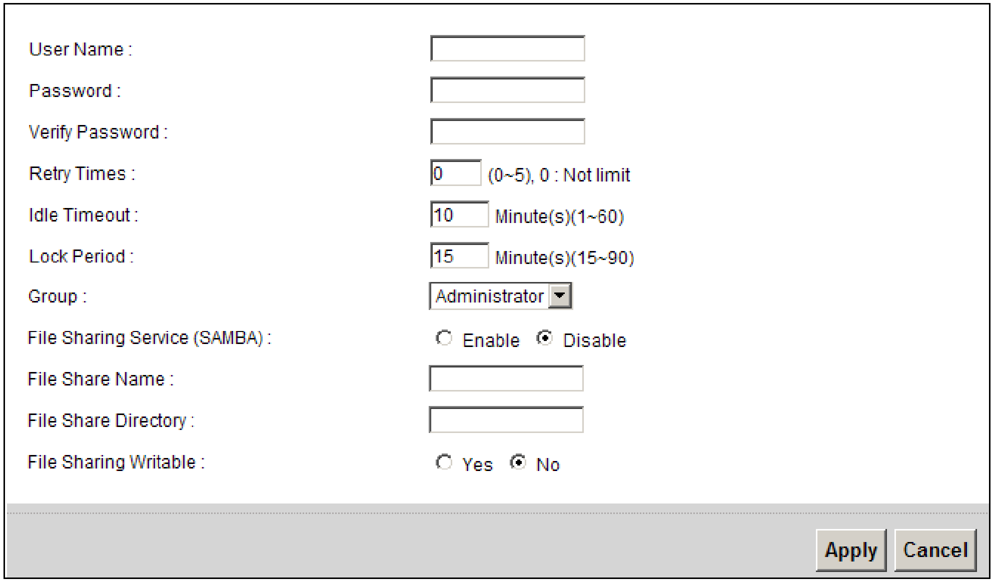
Table 114 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Lock Period	This field indicates the number of minutes for the lockout period. A user cannot log into the Device during the lockout period, even if he/she enters correct account information.
Group	This field displays the login account type of the user. Different login account types have different privilege levels. The web configurator screens and privileges vary depending on which account type you use to log in.
Modify	Click the **Edit** icon to edit this user account. Click the **Delete** icon to remove an account.
Web Captive Portal	Enable this feature to redirect each LAN host to the Device's login page for user authentication during its first connection to the Internet. The authentication time will be valid for 1 day after the user logs in successfully.
Customize Login Message	You can customize a message to display in the **Login** screen.

29.2.1 Add/Edit a User Account

Use this screen to add or edit a users account. Click **Add new user** in the **User Account** screen or the **Edit** icon next to the user account you want to edit. The screen shown next appears.

Figure 141 User Account: Add/Edit



User Name :	
Password :	
Verify Password :	
Retry Times :	0 (0~5), 0 : Not limit
Idle Timeout :	10 Minute(s)(1~60)
Lock Period :	15 Minute(s)(15~90)
Group :	Administrator
File Sharing Service (SAMBA) :	○ Enable ● Disable
File Share Name :	
File Share Directory :	
File Sharing Writable :	○ Yes ● No

The following table describes the labels in this screen.

Table 115 User Account: Add/Edit

LABEL	DESCRIPTION
User Name	This field is read-only if you are editing the user account. Enter a descriptive name for the user account. The user name can be up to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces). With advanced account security enabled, the user names must be a minimum length of six characters and include both letters and numbers.
Password	Specify the password associated to this account. The password can be 6 to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces), not containing the user name. It must contain both letters and numbers. The characters are displayed as asterisks (*) in this field.
Verify Password	Enter the exact same password that you just entered in the above field.
New Password	This field is displayed only when you are editing the user account. Type your new system password (6 to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces), not containing the user name).
Verify Password	This field is displayed only when you are editing the user account. Enter the exact same password that you just entered in the above field.
Retry Times	The Device can lock a user out if you use a wrong user name or password to log in the Device. Enter up to how many times a user can re-enter his/her account information before the Device locks the user out.
Idle Timeout	Enter the number of minutes that the system can idle before being logged out.
Lock Period	Enter the number of minutes for the lockout period. A user cannot log into the Device during the lockout period, even if he/she enters correct account information.
Group	This field is read-only if you are editing the user account. Select a type of login account. The web configurator screens and privileges vary depending on which account type you use to log in. **Administrator** accounts can configure the Device while **User** accounts can only view some status information. Users logged in with either type of account can access the Internet.
File Sharing Service (SAMBA)	Select **Enable** to allow the file sharing feature with this user account. This allows the user to access shared files in USB storage. Samba allows file and print sharing between computers running Windows and computers running Unix.
File Share Name	Enter a name for the shared resource (profile). For example, the user can connect to 192.168.1.1/<File Share Name>.
File Share Directory	Enter the shared root directory.
File Sharing Writable	Select if you want the files in the shared directory to be writable or not.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

30

Remote Management

30.1 Overview

Remote Management allows you to manage your SBG3500-N from a remote location through the following interfaces:

- LAN
- WAN
- Trust Domain

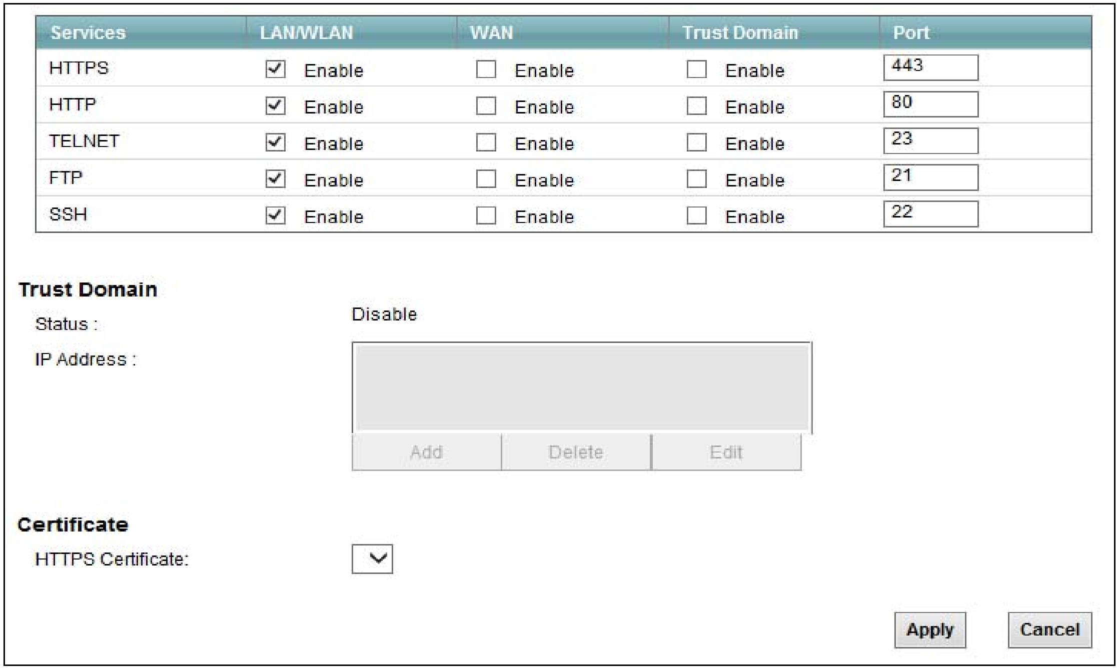
Note: The SBG3500-N is managed using the Web Configurator.

30.2 The Remote MGMT Screen

Use this screen to configure through which interface(s) users can use which service(s) to manage the SBG3500-N.

Click **Maintenance > Remote MGMT** to open the following screen.

Figure 142 Maintenance > Remote MGMT



Services	LAN/WLAN	WAN	Trust Domain	Port
HTTPS	☑ Enable	□ Enable	□ Enable	443
HTTP	☑ Enable	□ Enable	□ Enable	80
TELNET	☑ Enable	□ Enable	□ Enable	23
FTP	☑ Enable	□ Enable	□ Enable	21
SSH	☑ Enable	□ Enable	□ Enable	22

Trust Domain

Status : Disable

IP Address :

Certificate

HTTPS Certificate:

The following table describes the fields in this screen.

Table 116 Maintenance > Remote MGMT

LABEL	DESCRIPTION
Trust Domain	
Status	This field displays whether the Trust Domain is active or not.
IP Address	Enter the Trust Domain IP address.
Add	Click **Add** to add an IP address which the computer is allowed to access and manage the the SBG3500-N.
Delete	Click **Delete** to remove an IP address which the computer is not allowed to access and manage the the SBG3500-N.
Edit	Click **Edit** to make changes to the IP addresses which the computer is allowed to access and manage the the SBG3500-N.
Services	This is the service you may use to access the SBG3500-N.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the SBG3500-N from the LAN/WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the SBG3500-N from the WAN.
Trust Domain	Select the **Enable** check box for the corresponding services that you want to allow access to the SBG3500-N from the Trust Domain.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Certificate	
HTTPS Certificate	Select a certificate the HTTPS server (the SBG3500-N) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **Certificates** screen.
Apply	Click **Apply** to save your changes back to the SBG3500-N.
Cancel	Click **Cancel** to restore your previously saved settings.

31

TR-069 Client

31.1 Overview

This chapter explains how to configure the Device’s TR-069 auto-configuration settings.

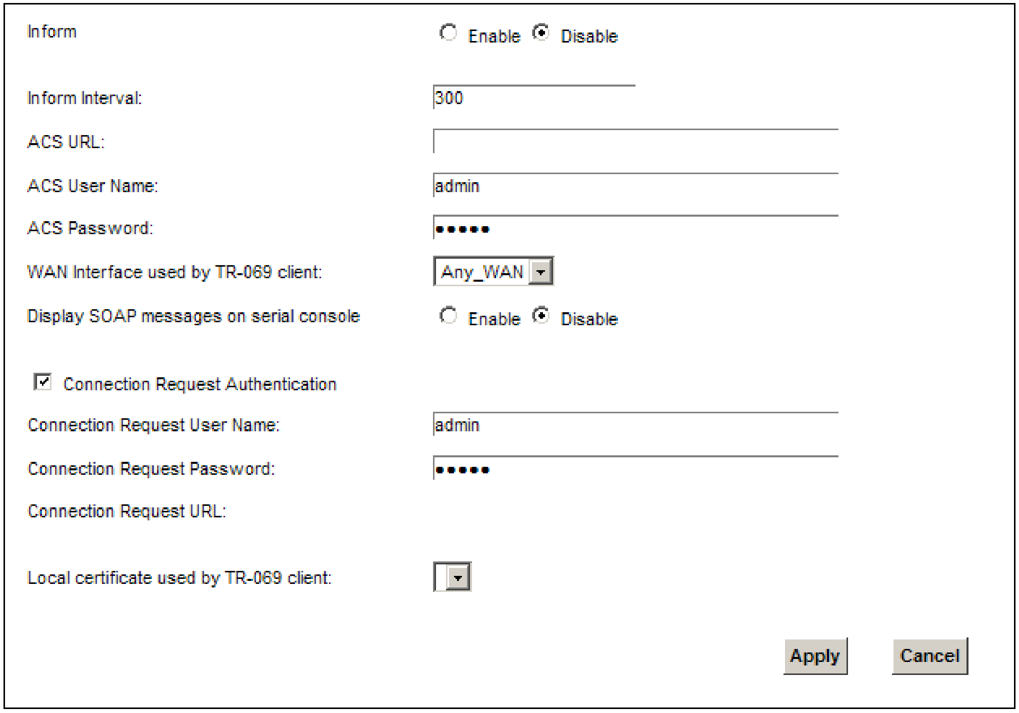
31.2 The TR-069 Client Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Device. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Maintenance > TR-069 Client** to open the following screen. Use this screen to configure your Device to be managed by an ACS.

Figure 143 Maintenance > TR-069 Client



Inform	○ Enable ● Disable
Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	•••••
WAN Interface used by TR-069 client:	Any_WAN
Display SOAP messages on serial console	○ Enable ● Disable
☑ Connection Request Authentication	
Connection Request User Name:	admin
Connection Request Password:	•••••
Connection Request URL:	
Local certificate used by TR-069 client:	

The following table describes the fields in this screen.

Table 117 Maintenance > TR-069 Client

LABEL	DESCRIPTION
Inform	Select **Enable** for the Device to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the Device sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select **Any_WAN**, you should also select the pre-configured WAN connection(s).
Display SOAP messages on serial console	Select **Enable** to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the Device, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the Device, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the Device.
Local certificate used by TR-069 client	You can choose a local certificate used by TR-069 client. The local certificate should be imported in the **Security** > **Certificates** > **Local Certificates** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

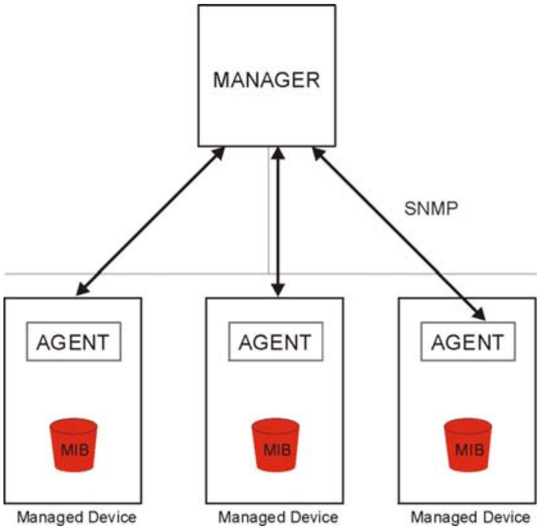
32

SNMP

32.1 The SNMP Agent Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Device through the network. The Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 144 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

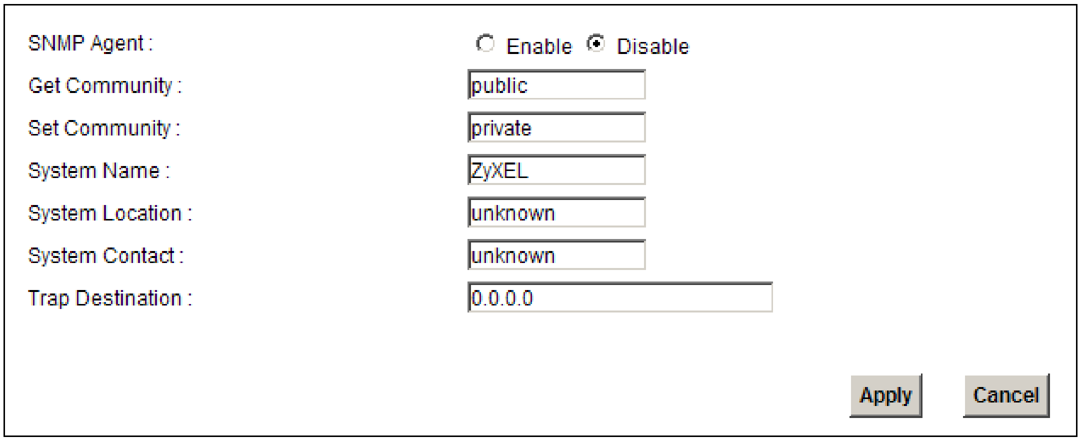
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

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

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the Device SNMP settings.

Figure 145 Maintenance > SNMP



SNMP Agent :	○ Enable ● Disable
Get Community :	public
Set Community :	private
System Name :	ZyXEL
System Location :	unknown
System Contact :	unknown
Trap Destination :	0.0.0.0

The following table describes the fields in this screen.

Table 118 Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Select **Enable** to allow a manager station to manage and monitor the Device through the network via SNMP. Otherwise, select **Disable**.
Get Community	Enter the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
System Name	Enter the system name of the Device.
System Location	Specify the geographic location of the Device.
System Contact	Enter the name of the person in charge of the Device.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click **Apply** to save your changes back to the Device.
Cancel	Click **Cancel** to restore your previously saved settings.

33

Time

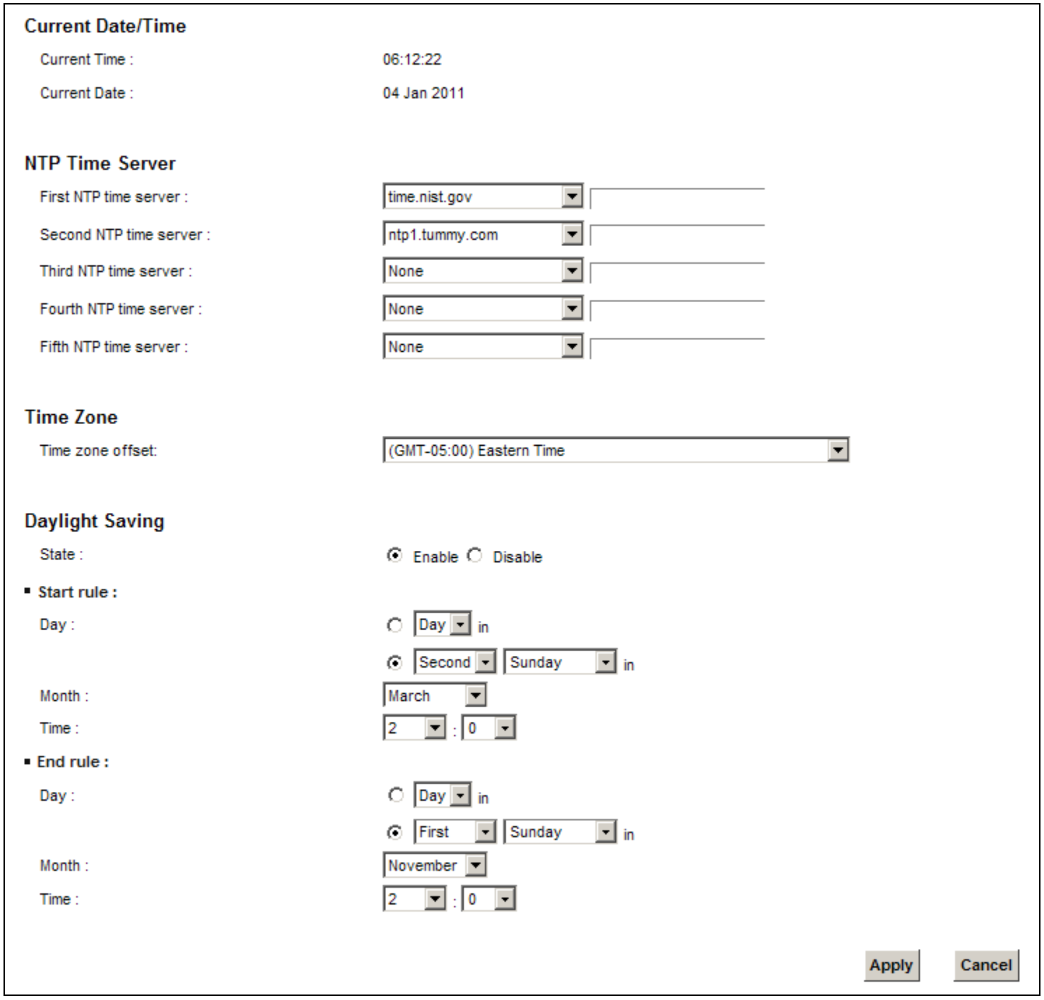
33.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

33.2 The Time Screen

To change your Device’s time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Device’s time based on your local time zone.

Figure 146 Maintenance > Time



Current Date/Time

Current Time :	06:12:22
Current Date :	04 Jan 2011

NTP Time Server

First NTP time server :	time.nist.gov
Second NTP time server :	ntp1.tummy.com
Third NTP time server :	None
Fourth NTP time server :	None
Fifth NTP time server :	None

Time Zone

Time zone offset:	(GMT-05:00) Eastern Time

Daylight Saving

State :	● Enable ○ Disable
▪ **Start rule :**	
Day :	○ Day in
	● Second Sunday in
Month :	March
Time :	2 : 0
▪ **End rule :**	
Day :	○ Day in
	● First Sunday in
Month :	November
Time :	2 : 0

The following table describes the fields in this screen.

Table 119 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your Device. Each time you reload this page, the Device synchronizes the time with the time server.
Current Date	This field displays the date of your Device. Each time you reload this page, the Device synchronizes the date with the time server.
NTP Time Server	
First ~ Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
State	Select **Enable** if you use Daylight Saving Time.
Start rule:	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 119 Maintenance > Time (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

34

E-mail Notification

34.1 Overview

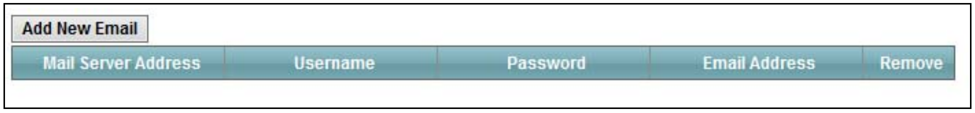
A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

34.2 The Email Notification Screen

Click **Maintenance > Email Notification** to open the **Email Notification** screen. Use this screen to view, remove and add mail server information on the Device.

Figure 147 Maintenance > Email Notification



The following table describes the labels in this screen.

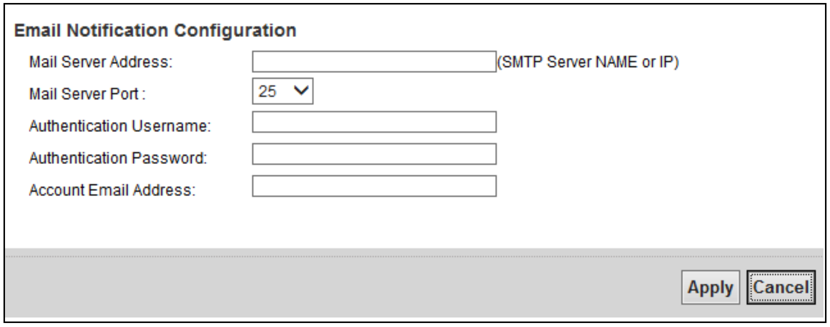
Table 120 Maintenance > Email Notification

LABEL	DESCRIPTION
Add New Email	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender’s mail account.
Password	This field displays the password of the sender’s mail account.
Email Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the Device sends.
Remove	Click this button to delete the selected entry(ies).

34.2.1 Email Notification Edit

Click the **Add** button in the **Email Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 148 Email Notification > Add



Email Notification Configuration

Mail Server Address: (SMTP Server NAME or IP)

Mail Server Port : 25

Authentication Username:

Authentication Password:

Account Email Address:

The following table describes the labels in this screen.

Table 121 Email Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account Email Address** field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Mail Server Port	Choose a mail server port **25** or **587** from the drop-down list. Choose Port 25 if you're using mail server from your ISP. Choose port 587 if you are using your own mailserver that is out of network with your ISP.
Authentication Username	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account Email Address** field.
Authentication Password	Enter the password associated with the user name above.
Account Email Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Device sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Apply	Click this button to save your changes and return to the previous screen.
Cancel	Click this button to begin configuring this screen afresh.

Logs Setting

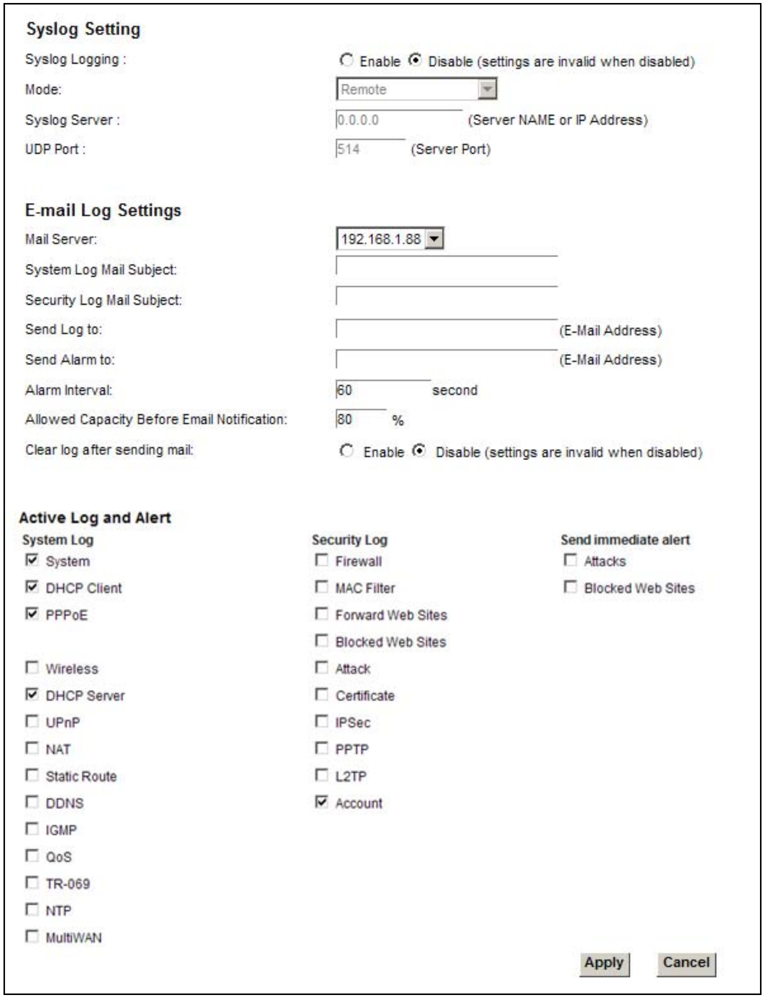
35.1 Overview

You can configure where the Device sends logs and which logs and/or immediate alerts the Device records in the **Logs Setting** screen.

35.2 The Log Setting Screen

To change your Device's log settings, click **Maintenance > Logs Setting**. The screen appears as shown.

Figure 149 Maintenance > Logs Setting



Syslog Setting

Syslog Logging : ○ Enable ● Disable (settings are invalid when disabled)

Mode: Remote

Syslog Server : 0.0.0.0 (Server NAME or IP Address)

UDP Port : 514 (Server Port)

E-mail Log Settings

Mail Server: 192.168.1.88

System Log Mail Subject:

Security Log Mail Subject:

Send Log to: (E-Mail Address)

Send Alarm to: (E-Mail Address)

Alarm Interval: 60 second

Allowed Capacity Before Email Notification: 80 %

Clear log after sending mail: ○ Enable ● Disable (settings are invalid when disabled)

Active Log and Alert

System Log

- ☑ System
- ☑ DHCP Client
- ☑ PPPoE
- □ Wireless
- ☑ DHCP Server
- □ UPnP
- □ NAT
- □ Static Route
- □ DDNS
- □ IGMP
- □ QoS
- □ TR-069
- □ NTP
- □ MultiWAN

Security Log

- □ Firewall
- □ MAC Filter
- □ Forward Web Sites
- □ Blocked Web Sites
- □ Attack
- □ Certificate
- □ IPSec
- □ PPTP
- □ L2TP
- ☑ Account

Send immediate alert

- □ Attacks
- □ Blocked Web Sites

The following table describes the fields in this screen.

Table 122 Maintenance > Logs Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The Device sends a log to an external syslog server. Select **Enable** to enable syslog logging.
Mode	Select the syslog destination from the drop-down list box. If you select **Remote**, the log(s) will be sent to a remote syslog server. If you select **Local File**, the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select **Local File and Remote**.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the Device sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the Device sends.
Send Log to	The Device sends logs to the e-mail address specified in this field. If this field is left blank, the Device does not send logs via E-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Alarm Interval	Specify how often the alarm should be updated.
Allowed Capacity Before Email	Set what percent of the Device’s log storage space can be filled before the Device sends a log e-mail.
Clear log after sending mail	Select this to delete all the logs after the Device sends an E-mail of the logs.
Active Log and Alert	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Send immediate alert	Select log categories for which you want the Device to send E-mail alerts immediately.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

35.2.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.

- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "`End of Log`" message shows that a complete log has been sent.

Figure 150 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
..................................{snip}.......................................
..................................{snip}.......................................
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

Firmware Upgrade

36.1 Overview

This chapter explains how to upload new firmware to your Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

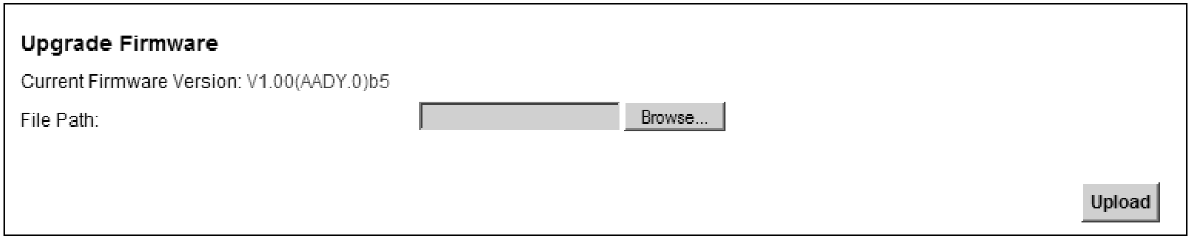
Only use firmware for your device's specific model. Refer to the label on the bottom of your Device.

36.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the Device while firmware upload is in progress!

Figure 151 Maintenance > Firmware Upgrade



Upgrade Firmware

Current Firmware Version: V1.00(AADY.0)b5

File Path:

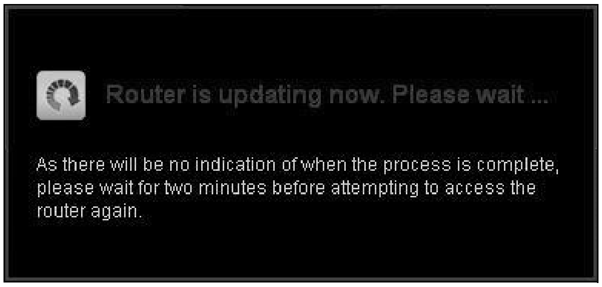
The following table describes the labels in this screen.

Table 123 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

After you see the firmware updating screen, wait two minutes before logging into the Device again.

Figure 152 Firmware Uploading

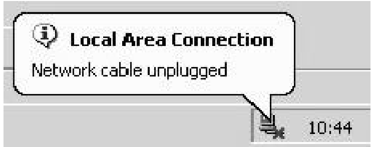


Router is updating now. Please wait ...

As there will be no indication of when the process is complete, please wait for two minutes before attempting to access the router again.

The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 153 Network Temporarily Disconnected



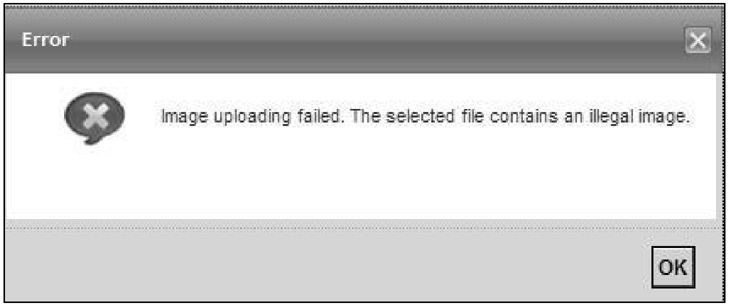
Local Area Connection

Network cable unplugged

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 154 Error Message



Error

Image uploading failed. The selected file contains an illegal image.

Configuration

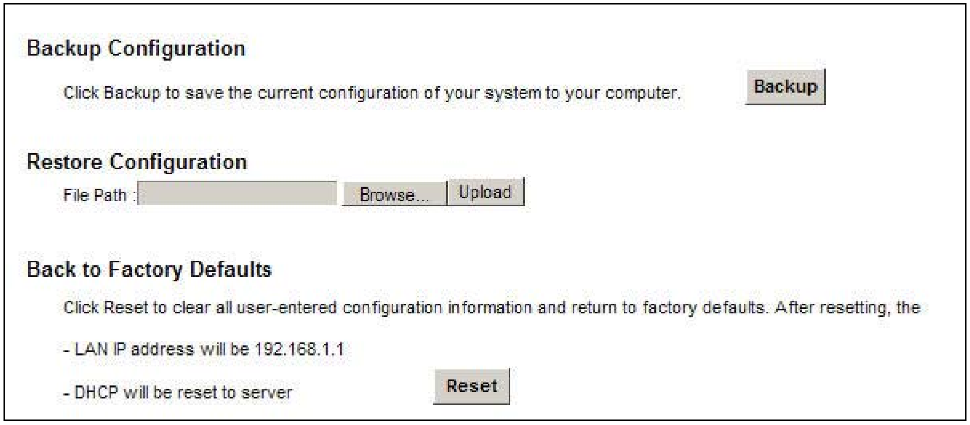
37.1 Overview

The **Configuration** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

37.2 The Configuration Screen

Click **Maintenance > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 155 Maintenance > Configuration



Backup Configuration

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

Restore Configuration

File Path :

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

Backup Configuration

Backup Configuration allows you to back up (save) the Device’s current configuration to a file on your computer. The configuration file should be saved and edited in UTF-8 (without BOM) format, if you’re using Windows Notepad, make sure you choose **File** > **Save as** UTF-8 in the text editor. Once your Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Device’s current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Device.

Table 124 Restore Configuration

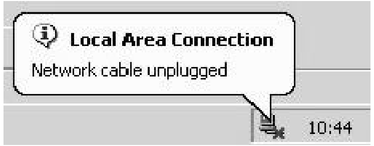
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the Device while configuration file upload is in progress.

After the Device configuration has been restored successfully, the login screen appears. Login again to restart the Device.

The Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 156 Network Temporarily Disconnected



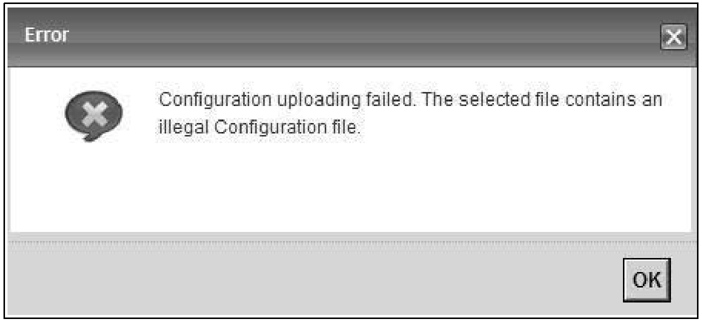
Local Area Connection

Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix A on page 334 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 157 Configuration Upload Error



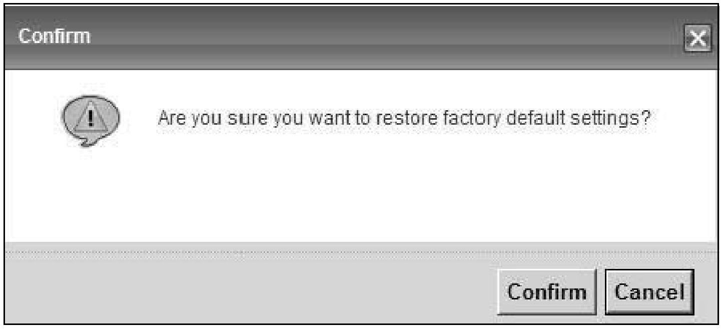
Error

Configuration uploading failed. The selected file contains an illegal Configuration file.

Reset to Factory Defaults

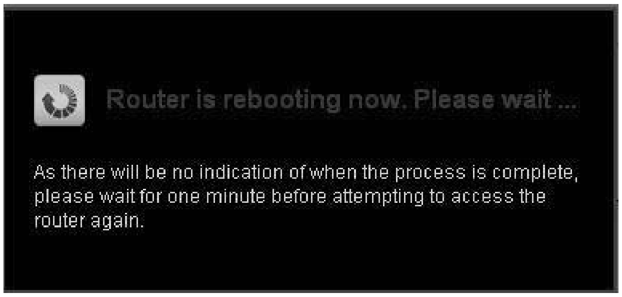
Click the **Reset** button to clear all user-entered configuration information and return the Device to its factory defaults. The following warning screen appears.

Figure 158 Reset Warning Message



Are you sure you want to restore factory default settings?

Figure 159 Reset In Process Message



Router is rebooting now. Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

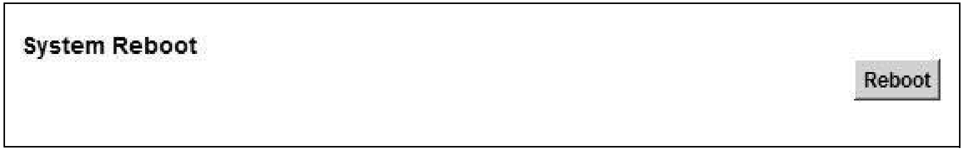
You can also press the **RESET** button on the rear panel to reset the factory defaults of your Device. Refer to Section 1.6 on page 24 for more information on the **RESET** button.

37.3 The Reboot Screen

System restart allows you to reboot the Device remotely without turning the power off. You may need to do this if the Device hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the Device reboot. This does not affect the Device's configuration.

Figure 160 Maintenance > Reboot



Diagnostic

38.1 Overview

The **Diagnostic** screens display information to help you identify problems with the Device.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

38.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets take to a host (Section 38.3 on page 323).
- The **802.1ag** screen lets you perform CFM actions (Section 38.5 on page 325).
- The **OAM Ping Test** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. (Section 38.5 on page 325).

38.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

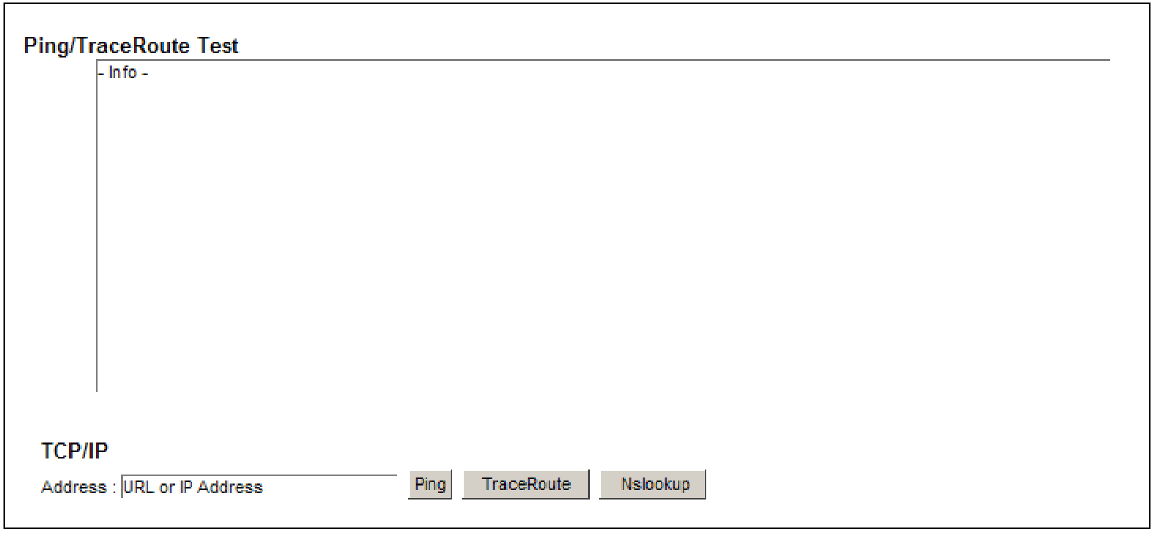
CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

38.3 Ping & TraceRoute & NsLookup

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic > Ping & TraceRoute & NsLookup** to open the screen shown next.

Figure 161 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup



The following table describes the fields in this screen.

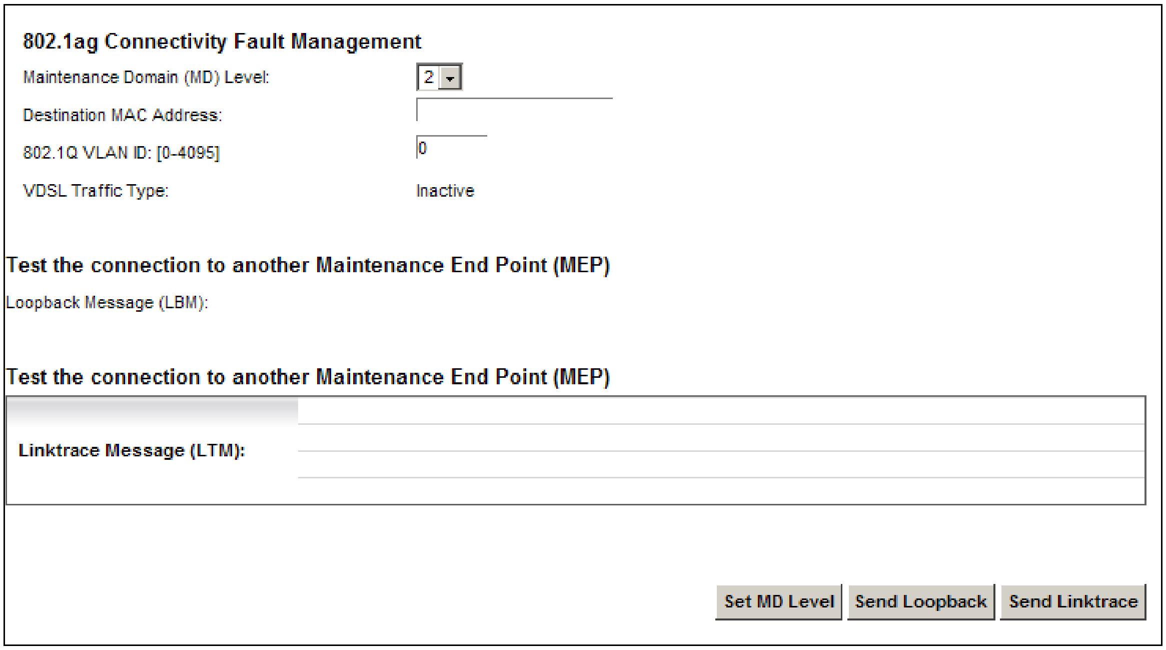
Table 125 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

LABEL	DESCRIPTION
URL or IP Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IP address that you entered.
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified computer.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

38.4 802.1ag

Click **Maintenance > Diagnostic** > **8.2.1ag** to open the following screen. Use this screen to perform CFM actions.

Figure 162 Maintenance > Diagnostic > 802.1ag



802.1ag Connectivity Fault Management

Maintenance Domain (MD) Level: 2

Destination MAC Address:

802.1Q VLAN ID: [0-4095] 0

VDSL Traffic Type: Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Test the connection to another Maintenance End Point (MEP)

Linktrace Message (LTM):

The following table describes the fields in this screen.

Table 126 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
Destination MAC Address	Enter the target device’s MAC address to which the Device performs a CFM loopback test.
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
VDSL Traffic Type	This shows whether the VDSL traffic is activated.
Loopback Message (LBM)	This shows how many Loop Back Messages (LBMs) are sent and if there is any inorder or outorder Loop Back Response (LBR) received from a remote MEP.
Linktrace Message (LTM)	This shows the destination MAC address in the Link Trace Response (LTR).
Set MD Level	Click this button to configure the MD (Maintenance Domain) level.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

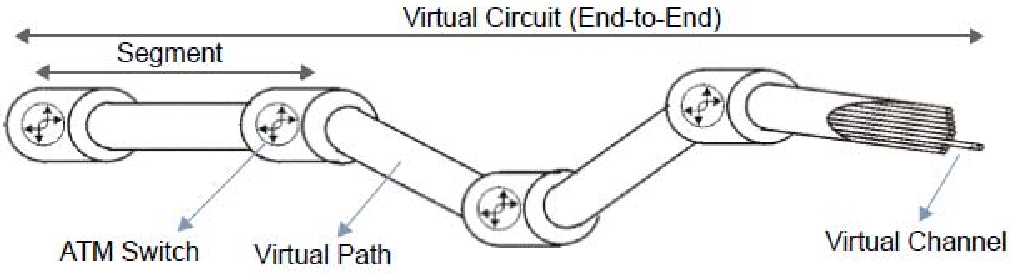
38.5 OAM Ping Test

Click **Maintenance > Diagnostic > OAM Ping Test** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The Device sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the Device. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

• Virtual Channel (VC)	Logical connections between ATM devices
• Virtual Path (VP)	A bundle of virtual channels
• Virtual Circuits	A series of virtual paths between circuit end points

Figure 163 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefinded Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

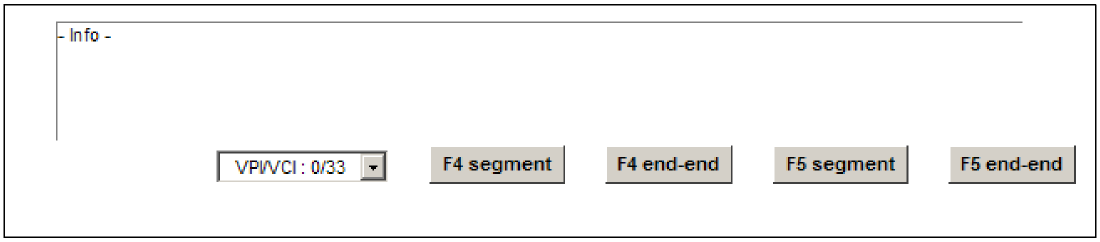
- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the Device is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 164 Maintenance > Diagnostic > OAM Ping Test



The following table describes the fields in this screen.

Table 127 Maintenance > Diagnostic > OAM Ping Test

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

39

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Device Access and Login
- Internet Access
- Wireless Internet Access
- USB Device Connection
- UPnP

39.1 Power, Hardware Connections, and LEDs

The Device does not turn on. None of the LEDs turn on.

1. Make sure the Device is turned on.
2. Make sure you are using the power adaptor or cord included with the Device.
3. Make sure the power adaptor or cord is connected to the Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.3 on page 22.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the Device off and on.

5 If the problem continues, contact the vendor.

39.2 Device Access and Login

I forgot the IP address for the Device.

1 The default LAN IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 24.

I forgot the password.

1 The default admin password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 24.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 8.2 on page 163), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.3 on page 22.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix C on page 364.

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).

5 Reset the device to its factory defaults, and try to access the Device with the default IP address. See Section 1.6 on page 24.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Device using another service, such as Telnet. If you can access the Device, check the remote management settings and firewall rules to find out why the Device does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Device.

1 Make sure you have entered the password correctly. The default admin password is **1234**. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the Device. Log out of the Device in the other session, or ask the person who is logged in to log out.

3 Turn the Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 39.1 on page 327.

I cannot Telnet to the Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

39.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.3 on page 22.

2 Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure that you enabled the wireless LAN in the Device and your wireless client and that the wireless settings in the wireless client are the same as the settings in the Device.

4 Disconnect all the cables from your device and reconnect them.

5 If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

1 Make sure you have the **DSL WAN** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).

2 Make sure you configured a proper DSL WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

3 Check that the LAN interface you are connected to is in the same interface group as the DSL connection (**Network Setting > Interface Group**).

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

I cannot connect to the Internet using a Ethernet connection.

1 Make sure you have the Ethernet WAN port connected to a MODEM or Router.

2 Make sure you configured a proper EthernetWAN interface (**Network Setting > Broadband > Multi-WAN** screen) with the Internet account information provided by your ISP and that it is enabled.

3 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting > Interface Group/VLAN**).

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot access the Internet anymore. I had access to the Internet (with the Device), but my Internet connection is not available anymore.

1 Your session with the Device may have expired. Try logging into the Device again.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.3 on page 22.

3 Turn the Device off and on.

4 If the problem continues, contact your ISP.

39.4 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.

- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

What wireless security modes does my Device support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your Device are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

39.5 USB Device Connection

The Device fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the Device.
3. Log into the web configurator and go to the **Maintenance** > **User Account** screen. Click the Edit icon on the account you are currently using. Check if the **File Sharing Service (SAMBA)** feature is enabled. You need to enable it to allow uses to access shared files in USB storage.
4. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

5 Re-connect your USB device to the Device.

39.6 UPnP

When using UPnP and the Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network.**

1 Disconnect the Ethernet cable from the Device’s LAN port or from your computer.

2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1 Wait more than three minutes.

2 Restart the applications.

A

Setting up Your Computer’s IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

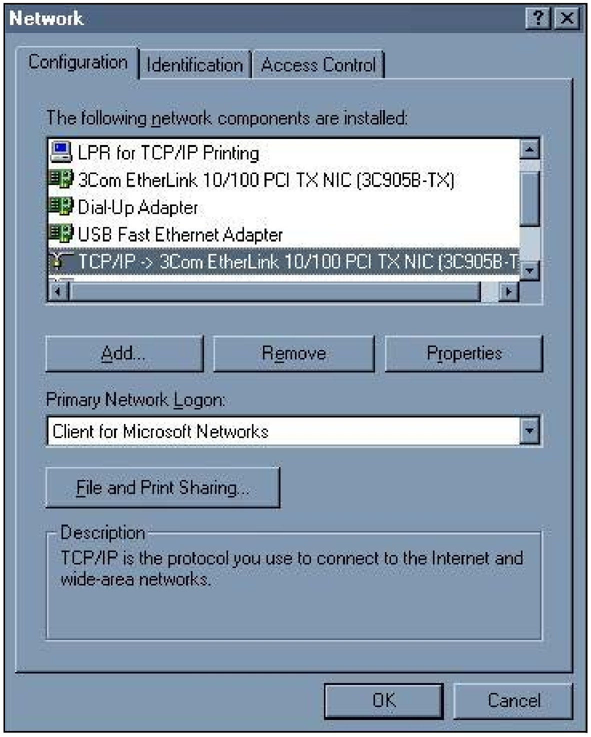
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Device’s LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 165 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon:

Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

Configuring

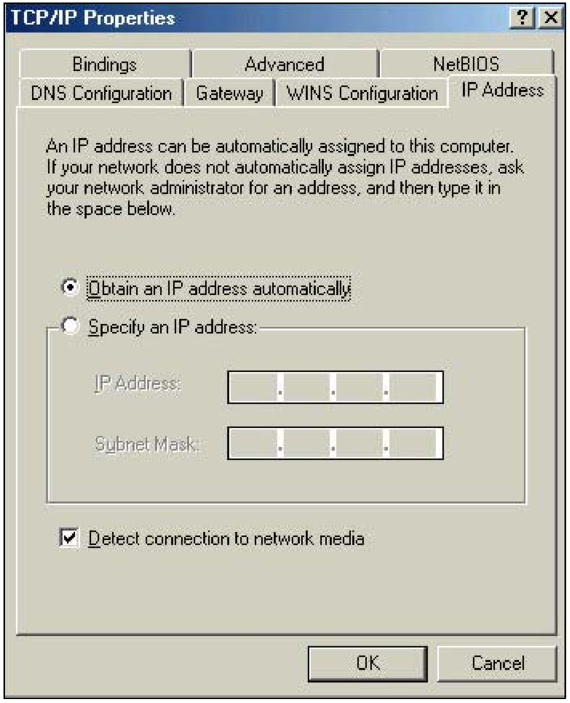
1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.

- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 166 Windows 95/98/Me: TCP/IP Properties: IP Address



TCP/IP Properties

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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

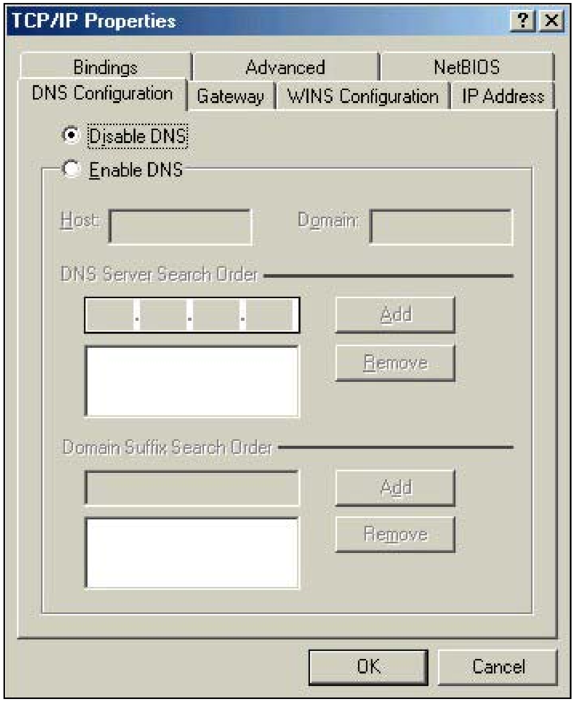
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 167 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



TCP/IP Properties

● Disable DNS

○ Enable DNS

Host:　Domain:

DNS Server Search Order

. . .

Domain Suffix Search Order

4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Device and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

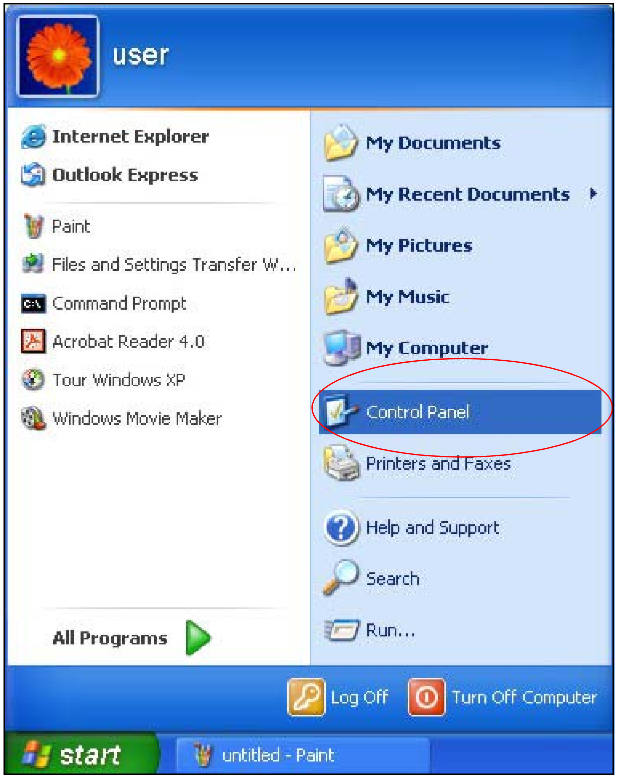
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

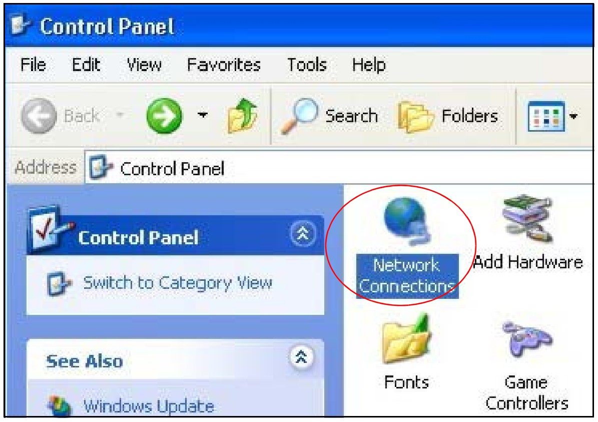
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 168 Windows XP: Start Menu



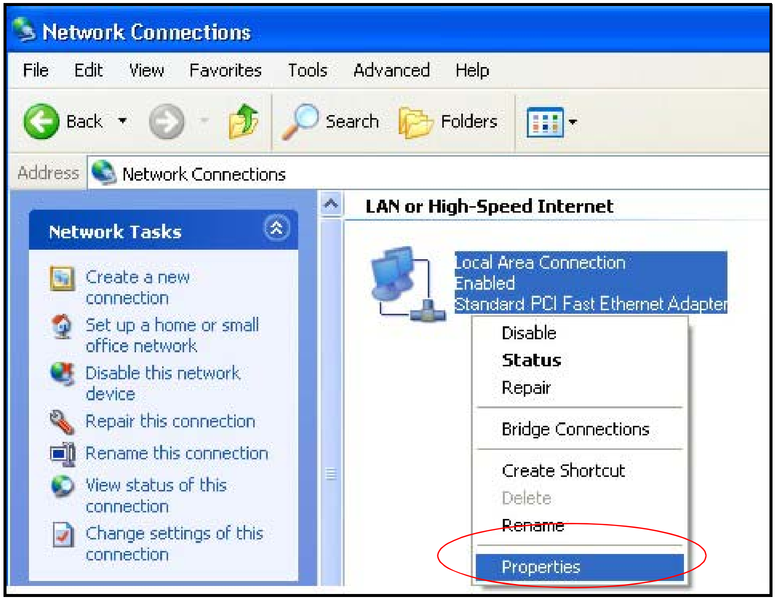
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 169 Windows XP: Control Panel



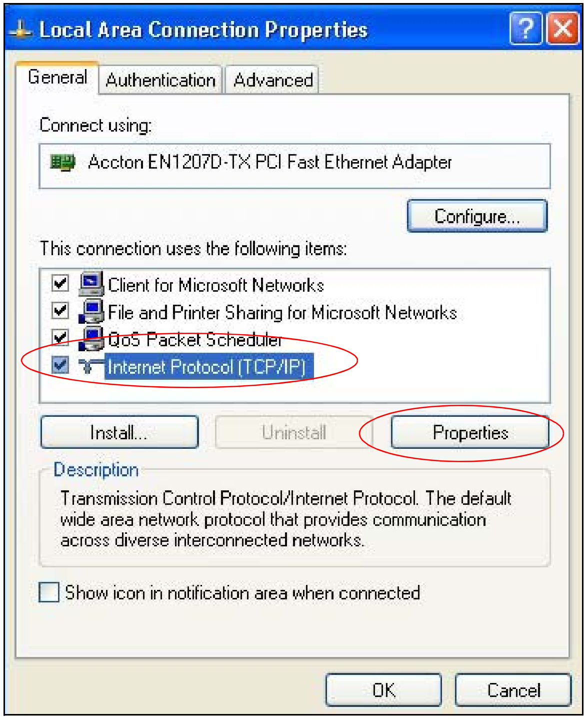
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 170 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 171 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

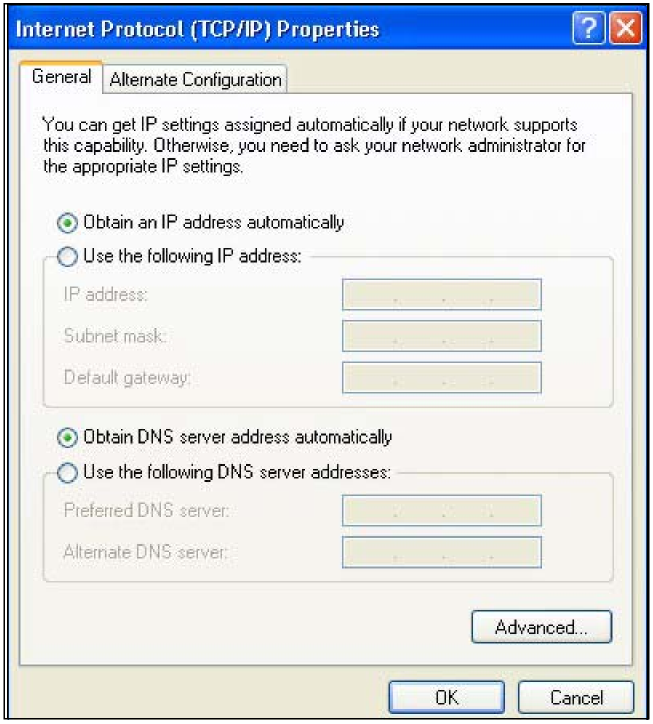
☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

Figure 172 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

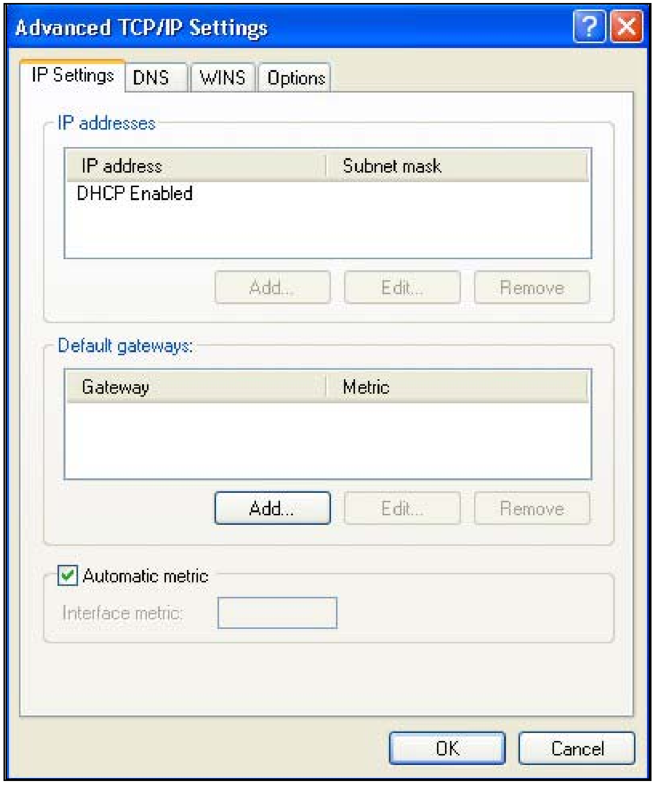
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

Figure 173 Windows XP: Advanced TCP/IP Properties



IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric

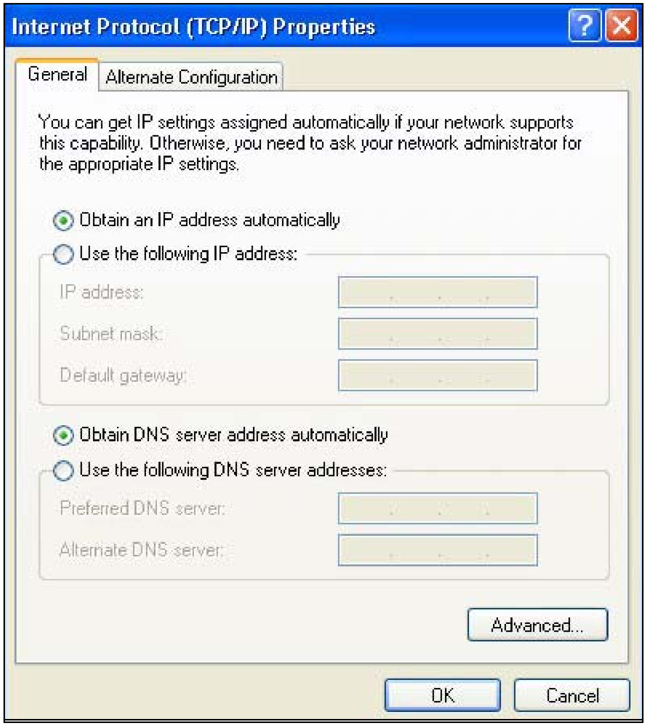
Interface metric:

7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 174 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your Device and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

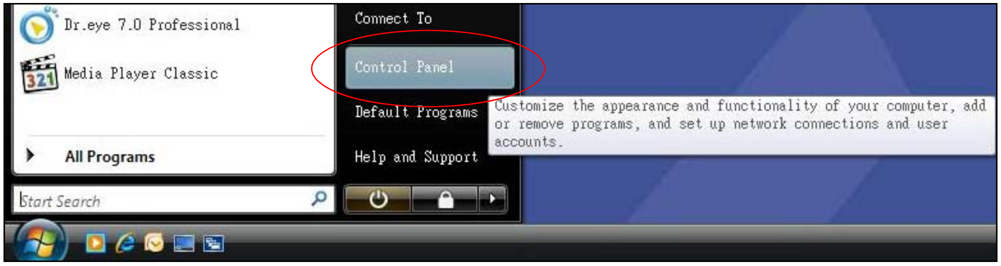
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

1 Click the **Start** icon, **Control Panel**.

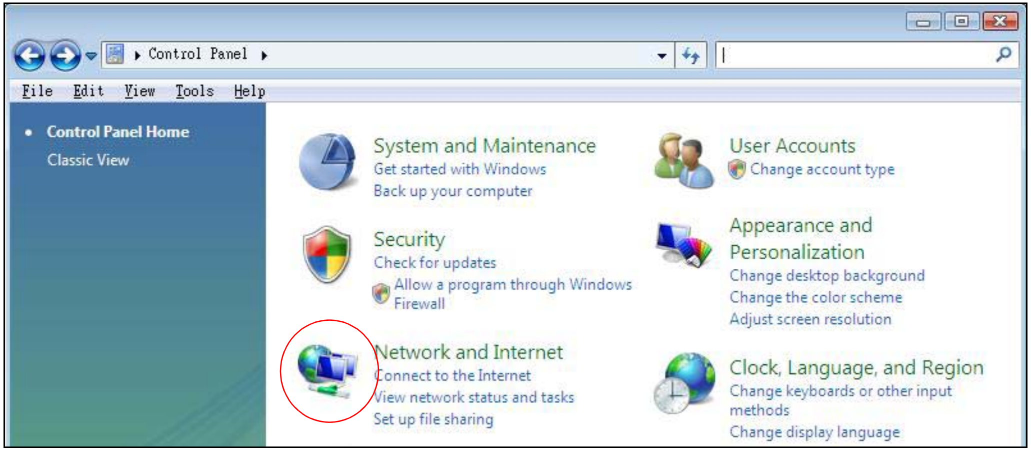
Figure 175 Windows Vista: Start Menu



Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

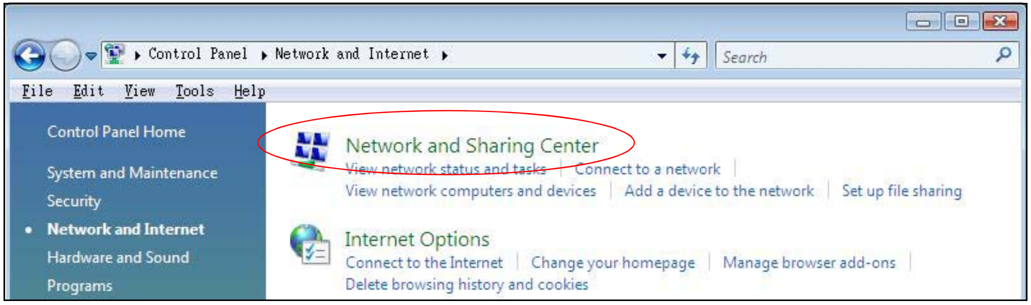
2 In the **Control Panel**, double-click **Network and Internet**.

Figure 176 Windows Vista: Control Panel



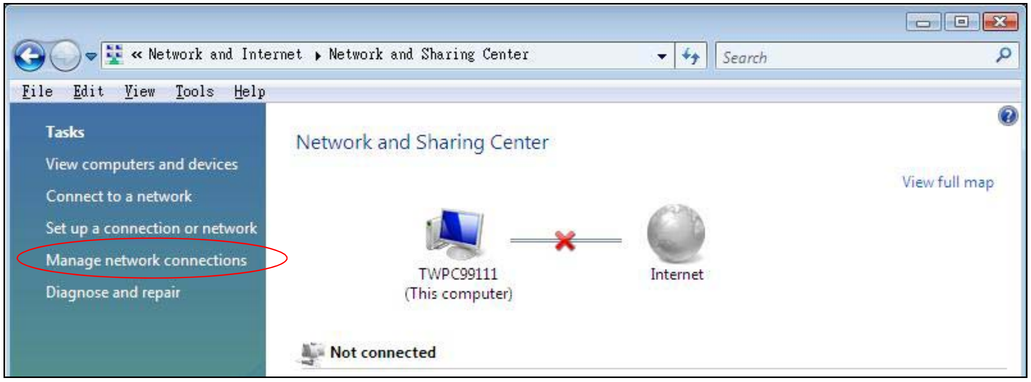
3 Click **Network and Sharing Center**.

Figure 177 Windows Vista: Network And Internet



4 Click **Manage network connections**.

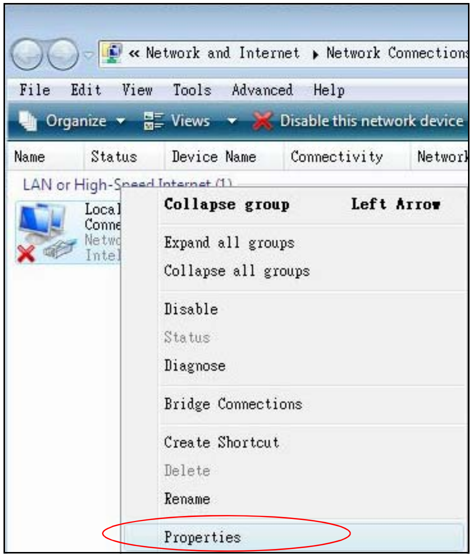
Figure 178 Windows Vista: Network and Sharing Center


« Network and Internet ▸ Network and Sharing Center
Search
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
View full map
TWPC99111
(This computer)
Internet
Not connected

5 Right-click **Local Area Connection** and then click **Properties**.

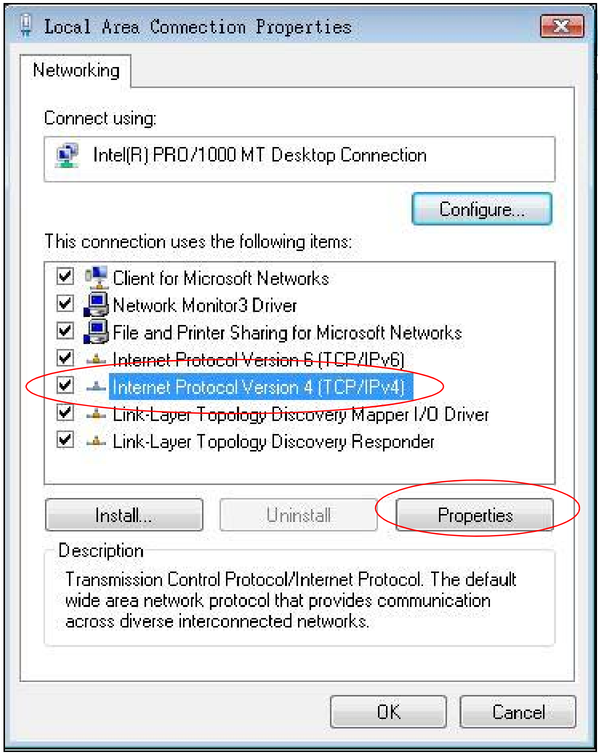
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 179 Windows Vista: Network and Sharing Center


« Network and Internet ▸ Network Connections
File Edit View Tools Advanced Help
Organize Views Disable this network device
Name Status Device Name Connectivity Network
LAN or High-Speed Internet (1)
Local Conne Netwo Intel
Collapse group Left Arrow
Expand all groups
Collapse all groups
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 180 Windows Vista: Local Area Connection Properties



Connect using:

Intel(R) PRO/1000 MT Desktop Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ Network Monitor3 Driver
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

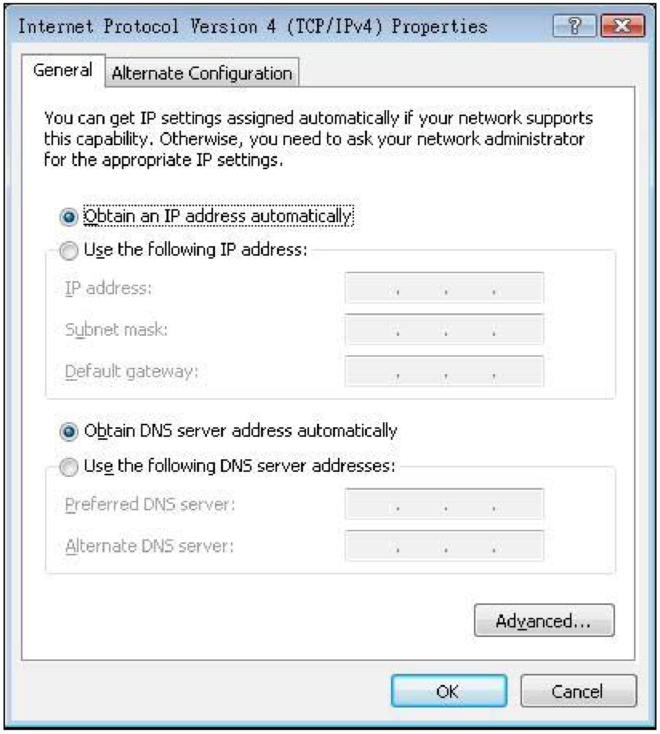
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

Figure 181 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

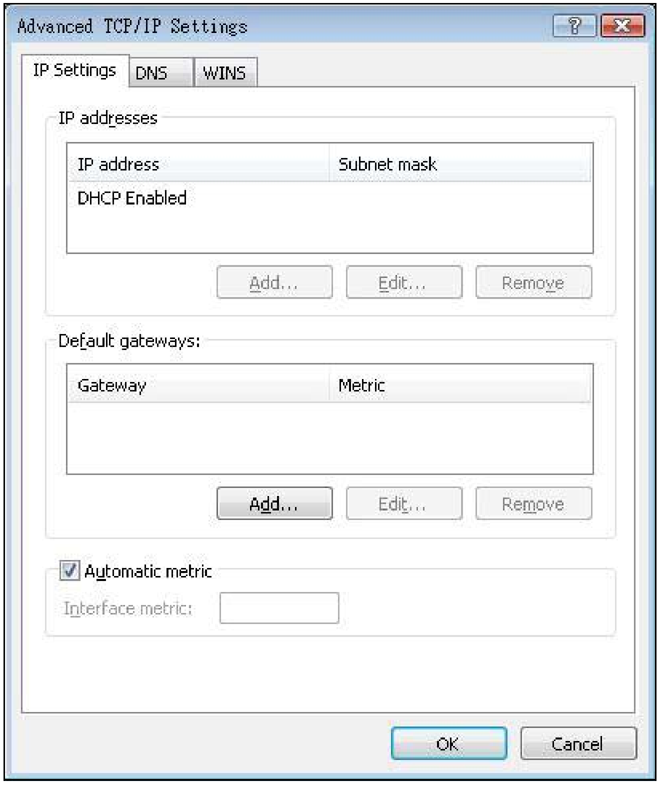
8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

Figure 182 Windows Vista: Advanced TCP/IP Properties



IP address	Subnet mask
DHCP Enabled	

Gateway	Metric

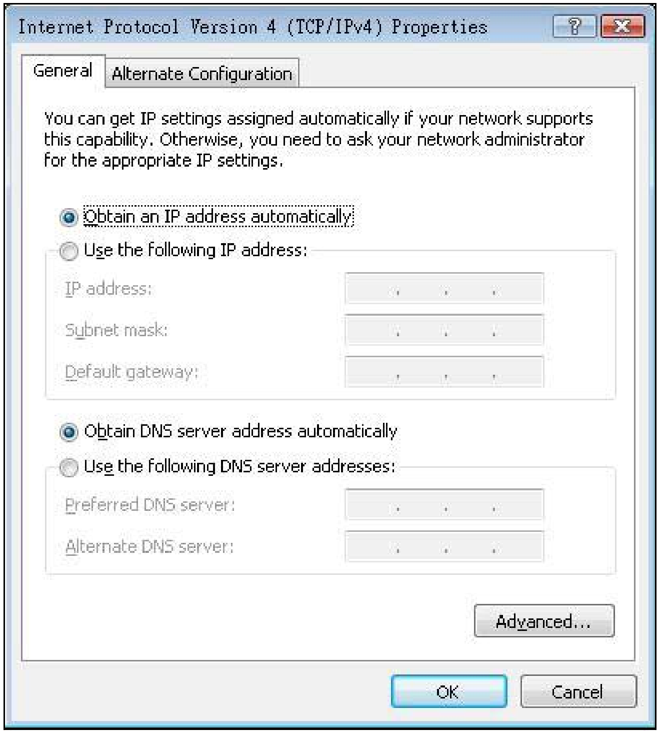
☑ Automatic metric

9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 183 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your Device and restart your computer (if prompted).

Verifying Settings

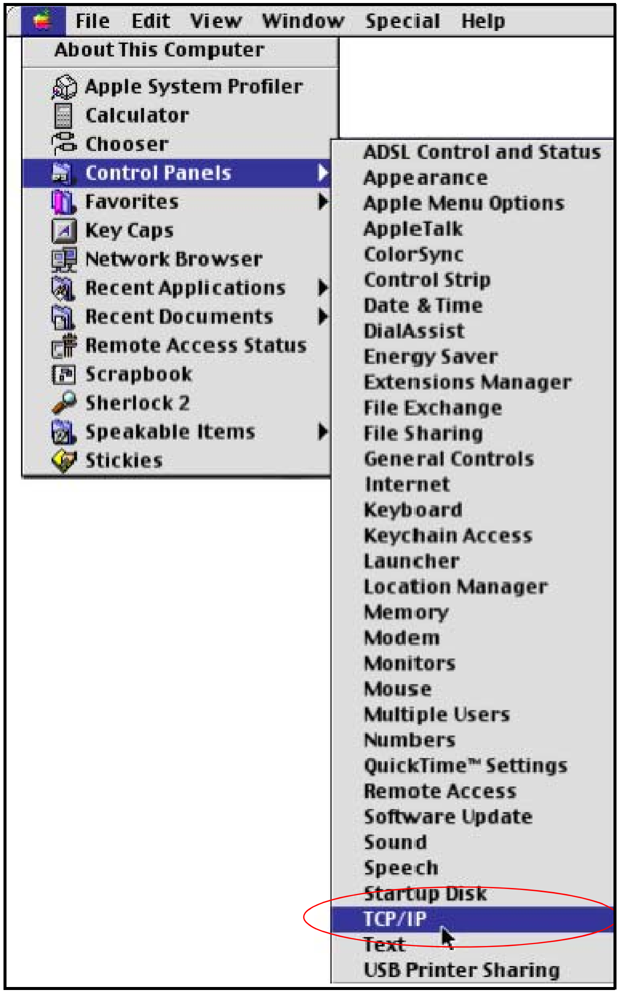
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

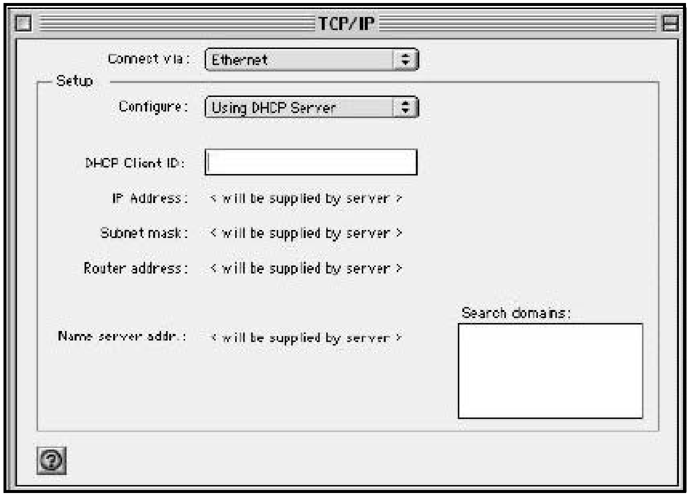
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 184 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 185 Macintosh OS 8/9: TCP/IP



Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Device and restart your computer (if prompted).

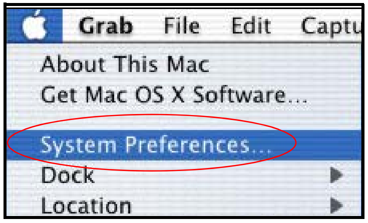
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 186 Macintosh OS X: Apple Menu



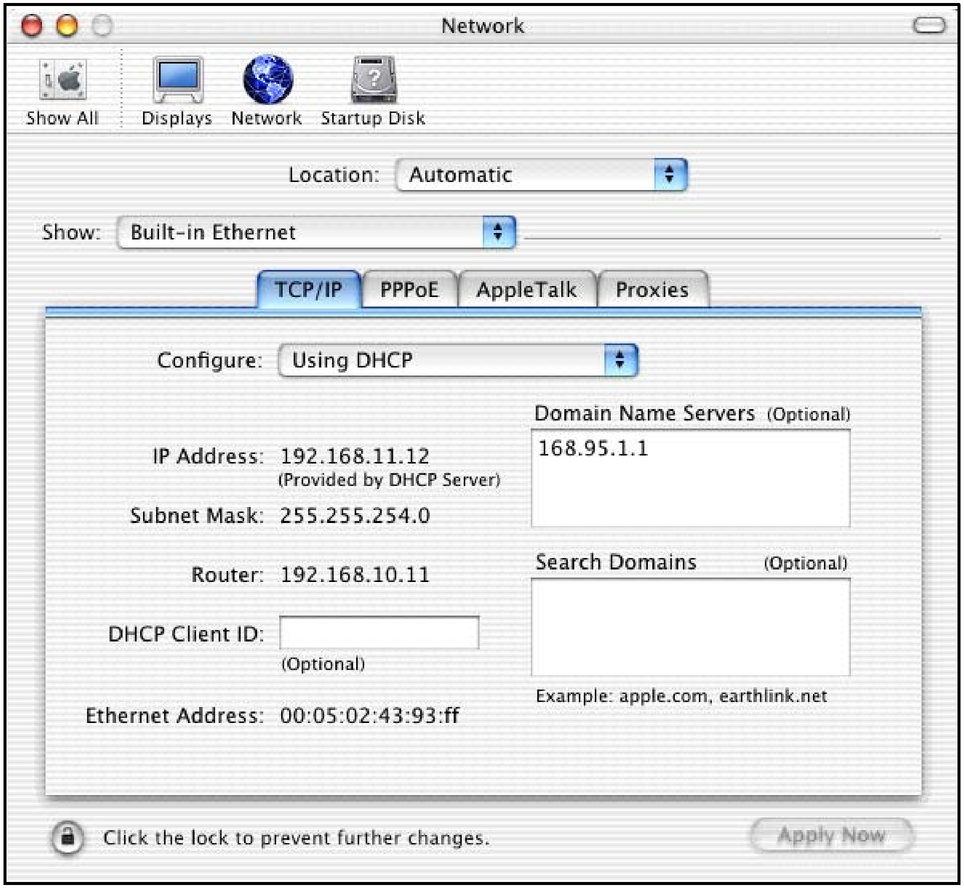
2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.

- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 187 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

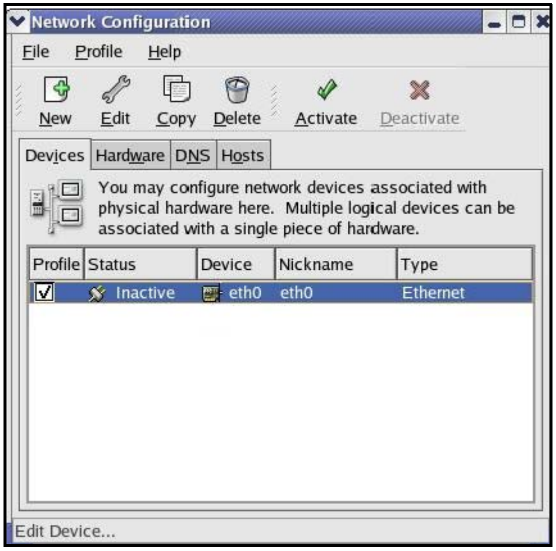
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 188 Red Hat 9.0: KDE: Network Configuration: Devices

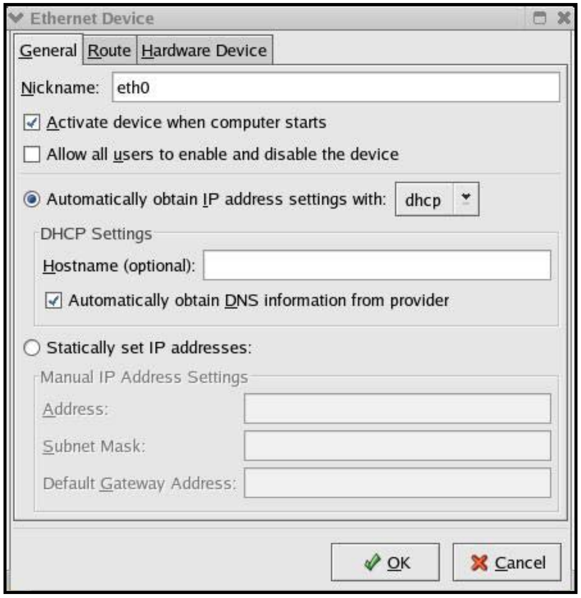


You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 189 Red Hat 9.0: KDE: Ethernet Device: General



Ethernet Device

Nickname: eth0

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

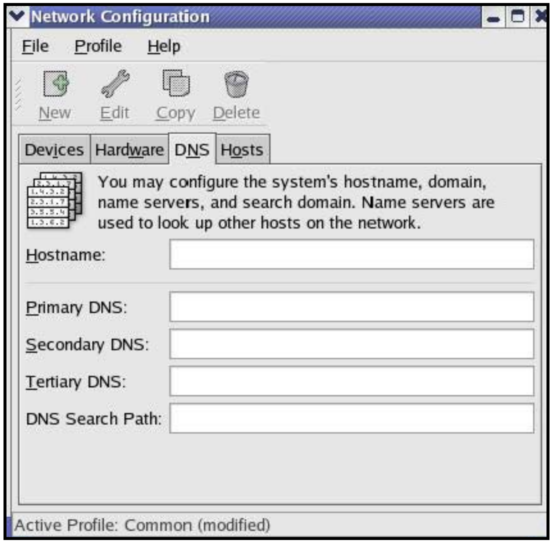
Default Gateway Address:

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop-down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 190 Red Hat 9.0: KDE: Network Configuration: DNS



Network Configuration

You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

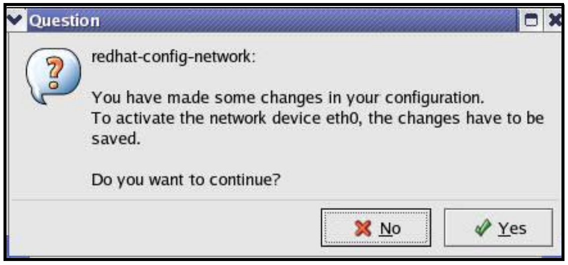
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 191 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 192 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 193 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 194 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 195 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                 [OK]
Shutting down loopback interface:             [OK]
Setting network parameters:                   [OK]
Bringing up loopback interface:               [OK]
Bringing up interface eth0:                   [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 196 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

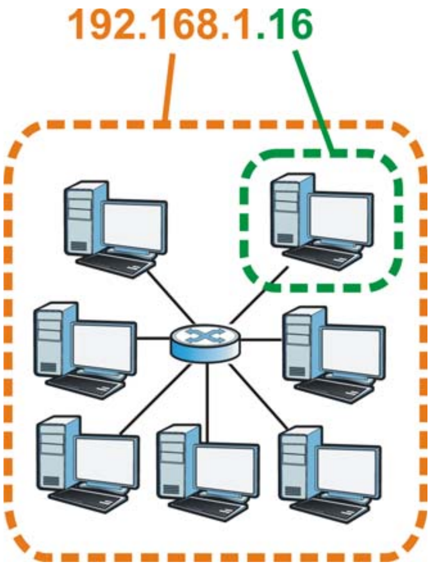
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 197 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 128 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 129 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 130 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 131 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

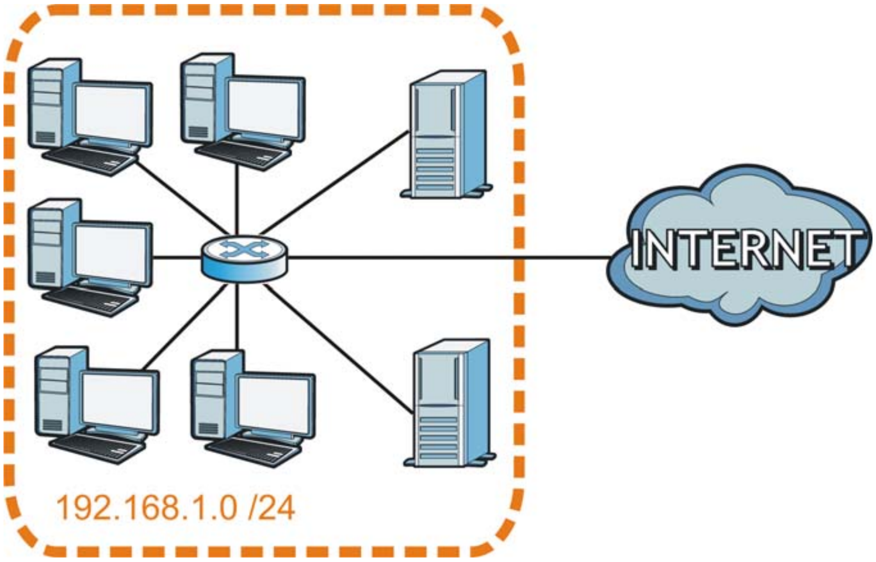
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 198 Subnetting Example: Before Subnetting

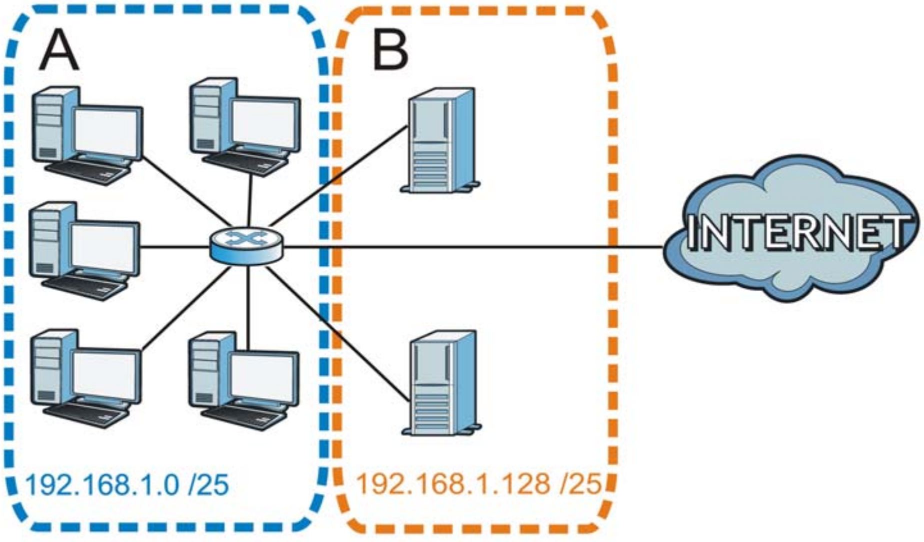


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 199 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 132 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 132 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 133 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 134 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 135 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 136 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63

Table 136 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 137 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 138 16-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Device.

Once you have decided on the network number, pick an IP address for your Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

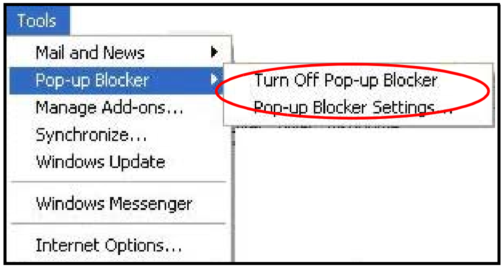
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 200 Pop-up Blocker

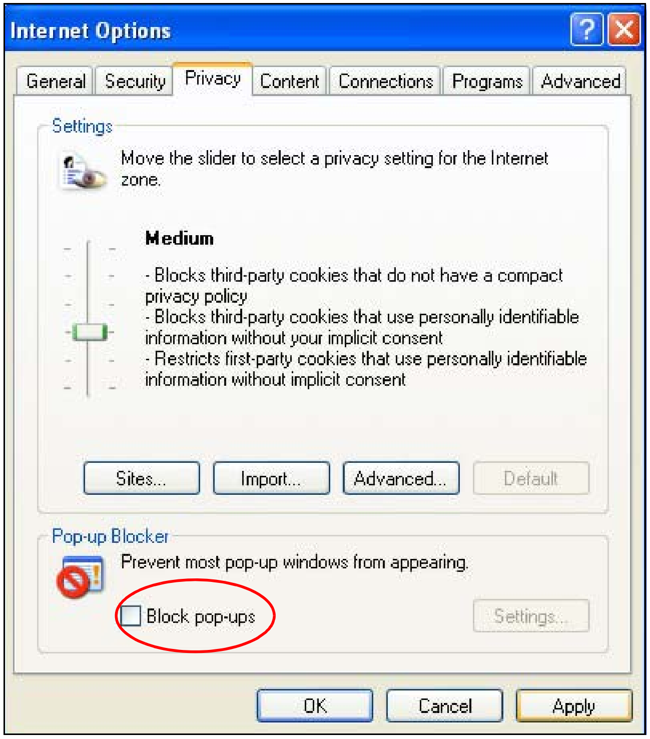


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 201 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☐ Block pop-ups

3 Click **Apply** to save this setting.

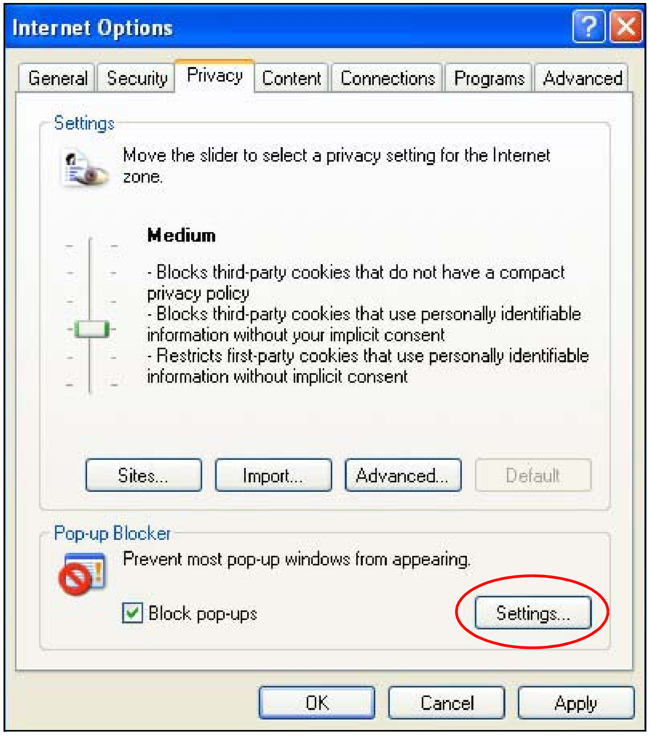
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 202 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

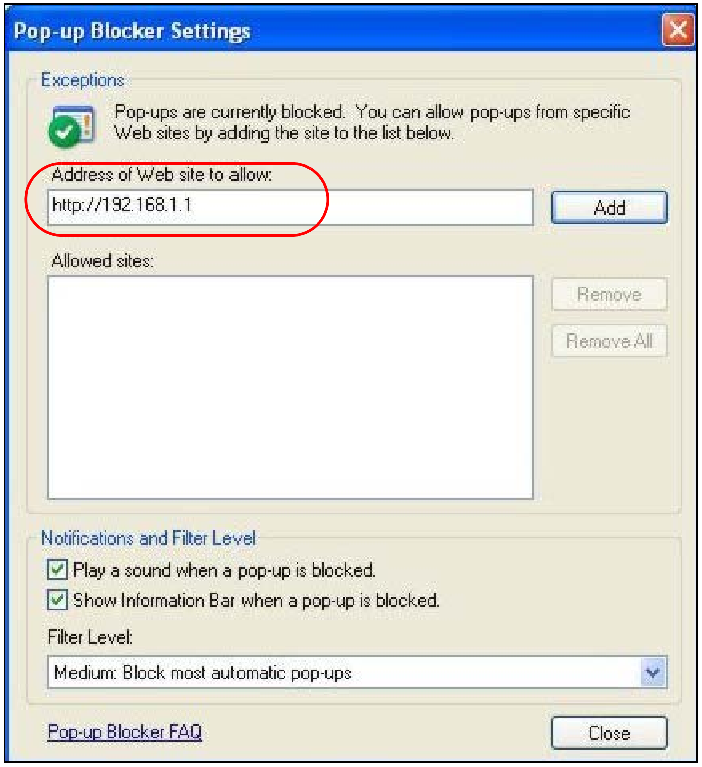
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 203 Pop-up Blocker Settings



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:

http://192.168.1.1

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level:

Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

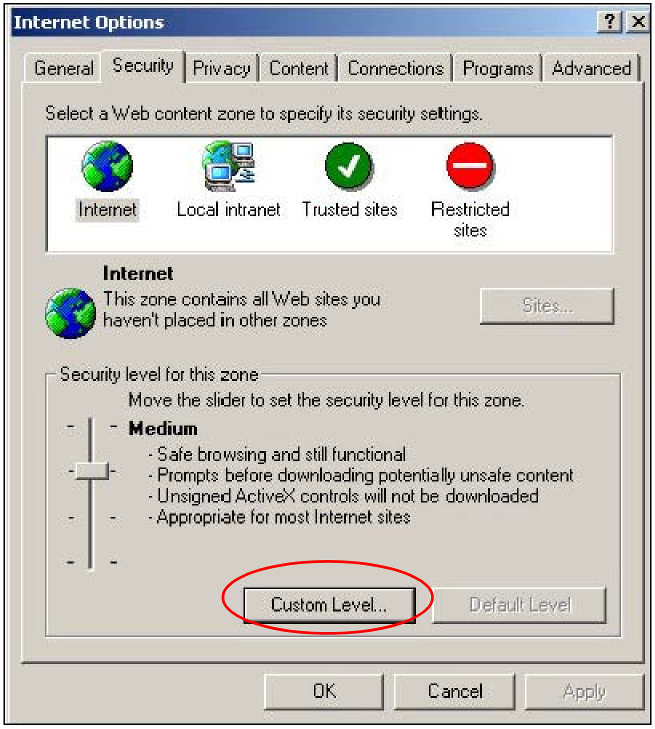
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 204 Internet Options: Security



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a Web content zone to specify its security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Internet
This zone contains all Web sites you haven't placed in other zones

Sites...

Security level for this zone

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

Custom Level... | Default Level

OK | Cancel | Apply

2 Click the **Custom Level...** button.

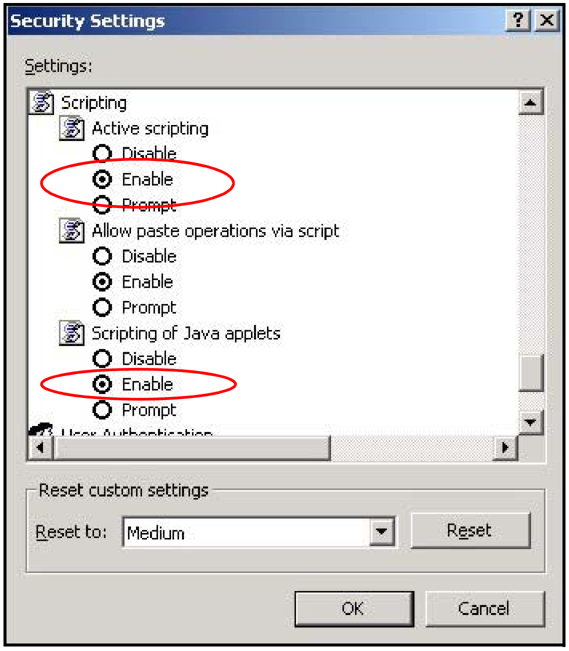
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 205 Security Settings - Java Scripting



Scripting
- Active scripting
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Allow paste operations via script
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Scripting of Java applets
  - ○ Disable
  - ● Enable
  - ○ Prompt

User Authentication

Reset to: Medium

Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

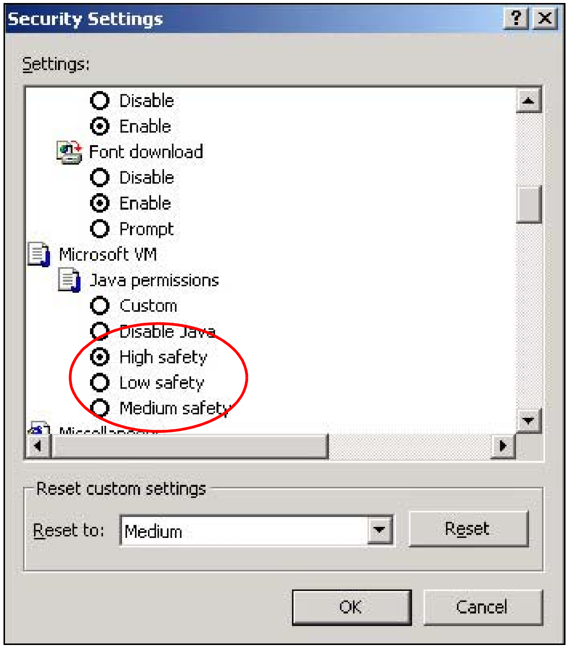
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 206 Security Settings - Java



Security Settings

Settings:

○ Disable
● Enable

Font download

○ Disable
● Enable
○ Prompt

Microsoft VM

Java permissions

○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

Reset custom settings

Reset to: Medium

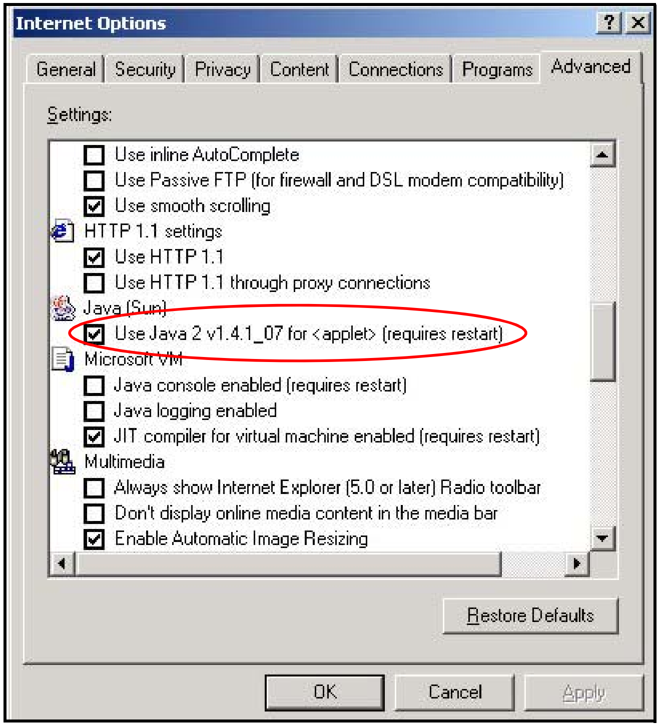
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 207 Java (Sun)



Settings:

- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- □ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- □ Java console enabled (requires restart)
- □ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

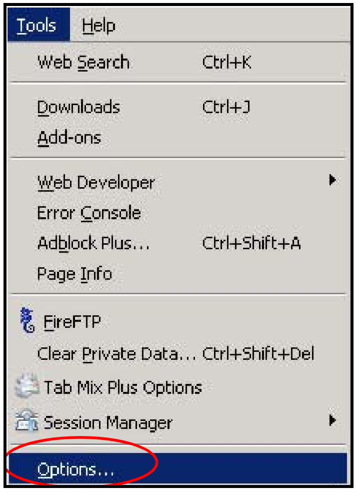
- □ Always show Internet Explorer (5.0 or later) Radio toolbar
- □ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

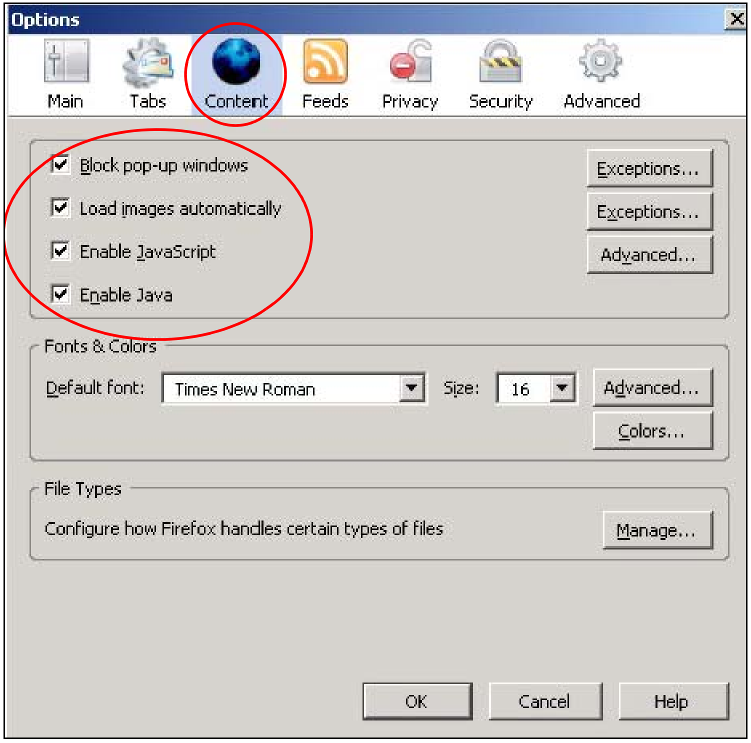
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 208 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 209 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman Size: 16

File Types

Configure how Firefox handles certain types of files

D

Wireless LANs

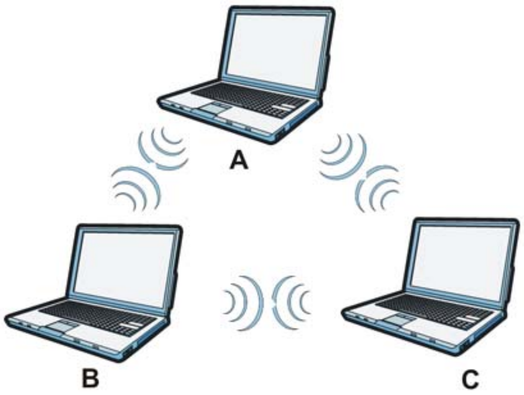
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 210 Peer-to-Peer Communication in an Ad-hoc Network

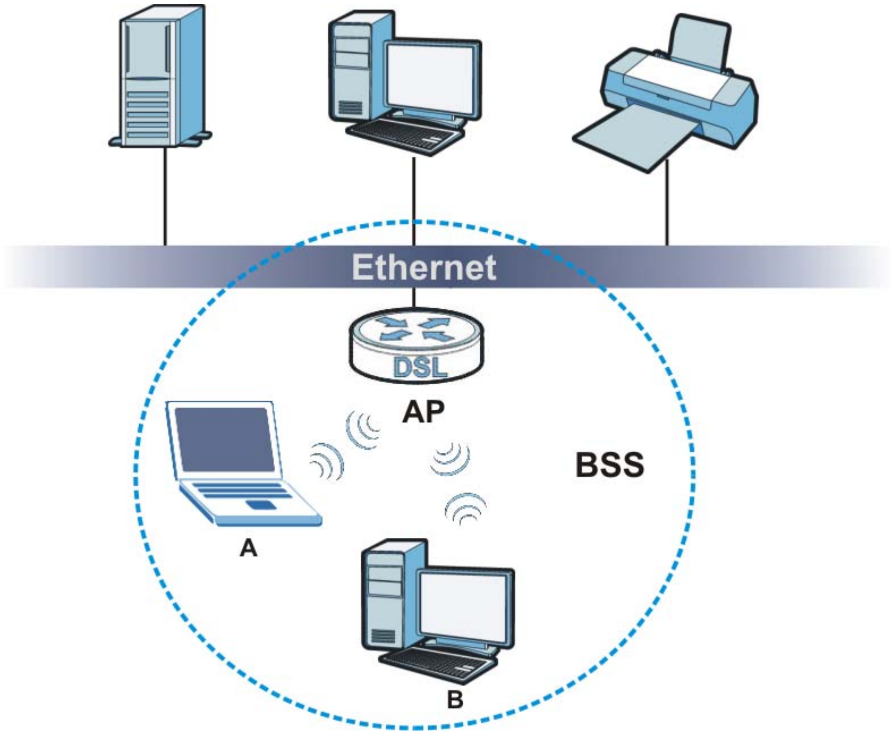


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 211 Basic Service Set



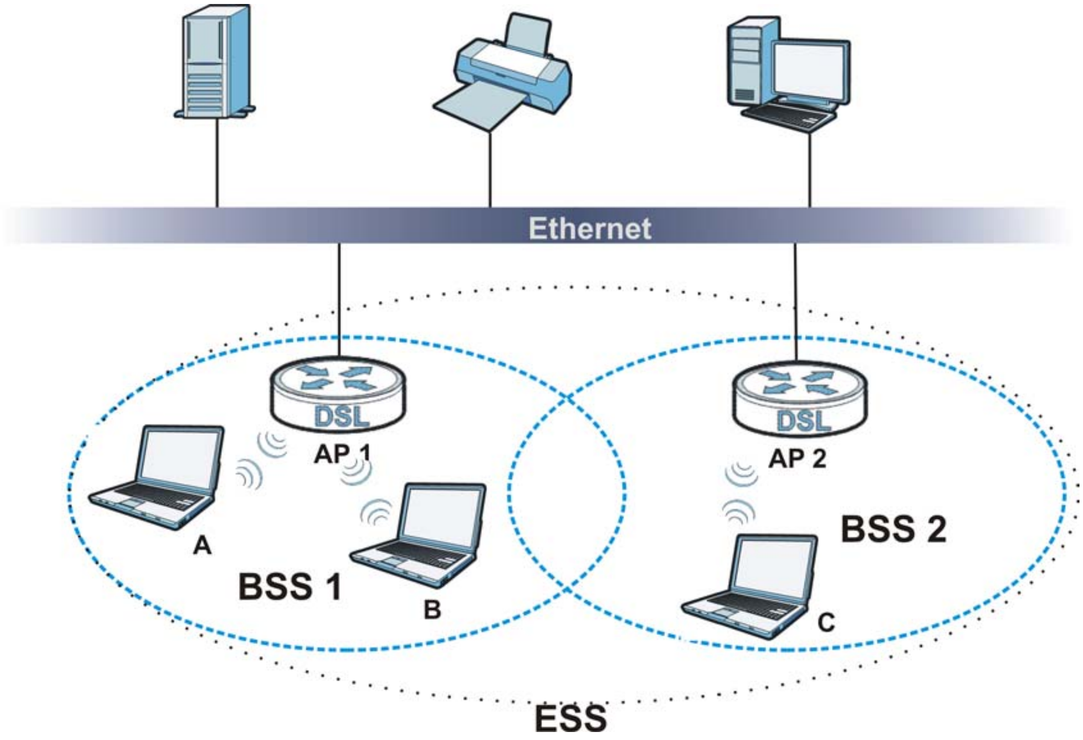
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 212 Infrastructure WLAN



Channel

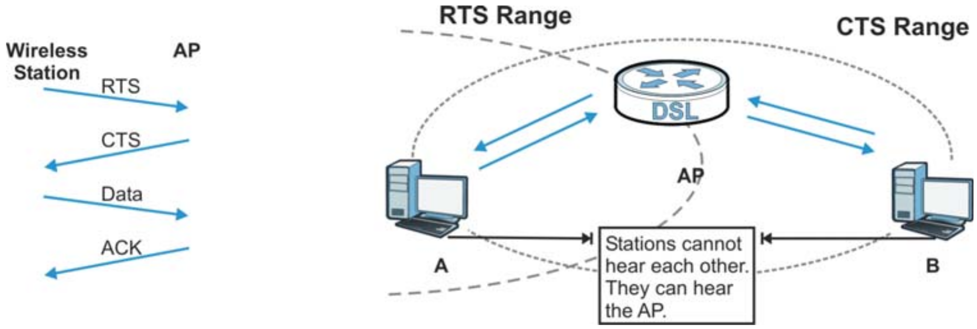
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 213 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 139 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Device.

Table 140 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client’s network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 141 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared 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 wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice. .

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

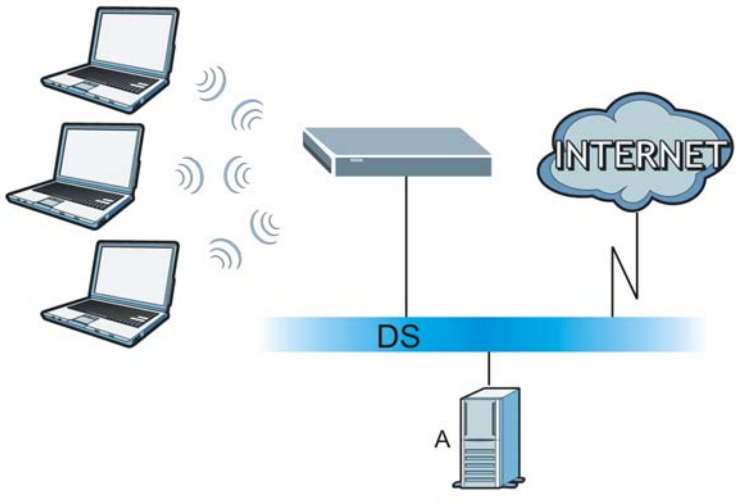
1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 214 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

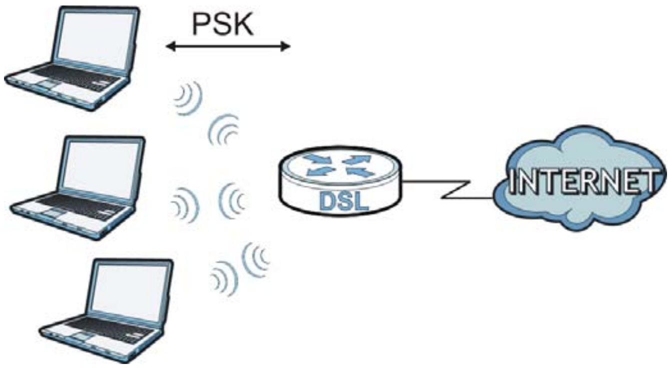
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 215 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 142 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTIO N METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna’s coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately

2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 143 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 144 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 145 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0

Table 145 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block’s 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

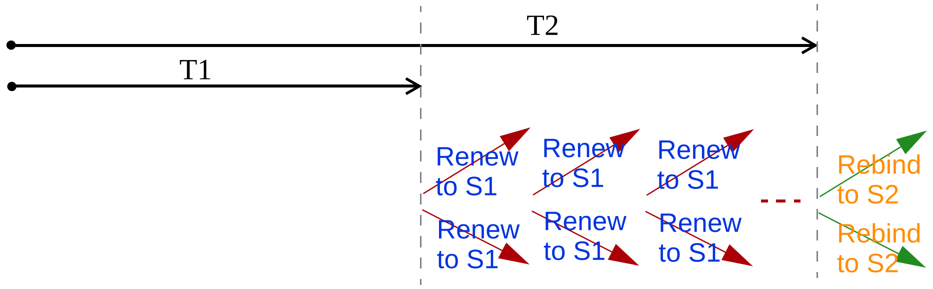
The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC	00 : 13 : 49 : 12 : 34 : 56
EUI-64	02 : 13 : 49 : FF : FE : 12 : 34 : 56

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor’s reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor’s link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being “reachable” means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.

- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Device also sends out a neighbor solicitation message. When the Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Device creates an entry in the default router list cache if the router can be used as a default router.

When the Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

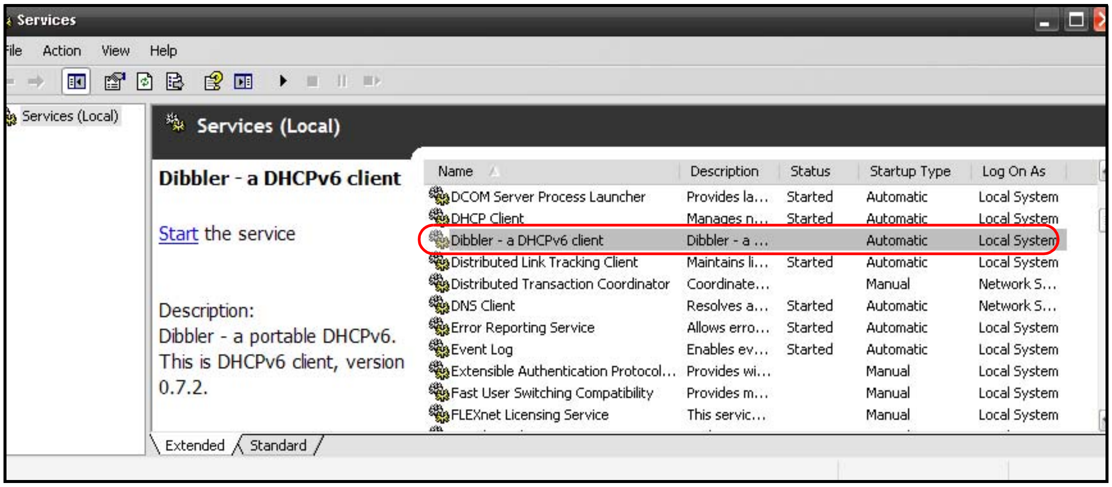
Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1. Install Dibbler and select the DHCPv6 client option on your computer.
2. After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



Services (Local)

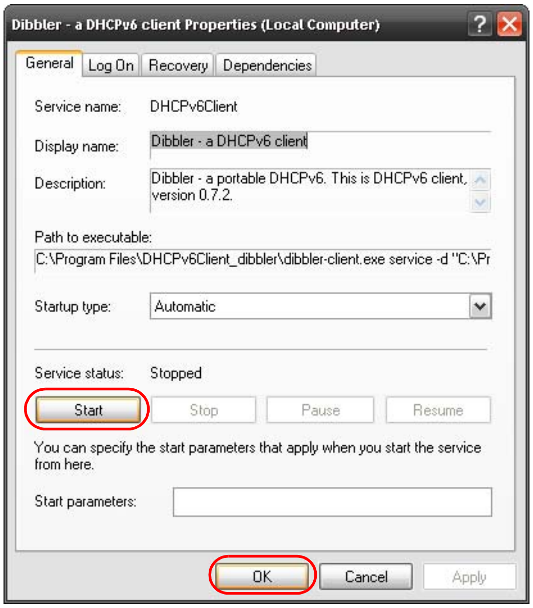
Dibbler - a DHCPv6 client

Start the service

Description:
Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Dibbler - a DHCPv6 client	Dibbler - a ...		Automatic	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Extensible Authentication Protocol...	Provides wi...		Manual	Local System
Fast User Switching Compatibility	Provides m...		Manual	Local System
FLEXnet Licensing Service	This servic...		Manual	Local System

5 Click **Start** and then **OK**.



Service name: DHCPv6Client

Display name: Dibbler - a DHCPv6 client

Description: Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Path to executable:
C:\Program Files\DHCPv6Client_dibbler\dibbler-client.exe service -d "C:\Pr

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

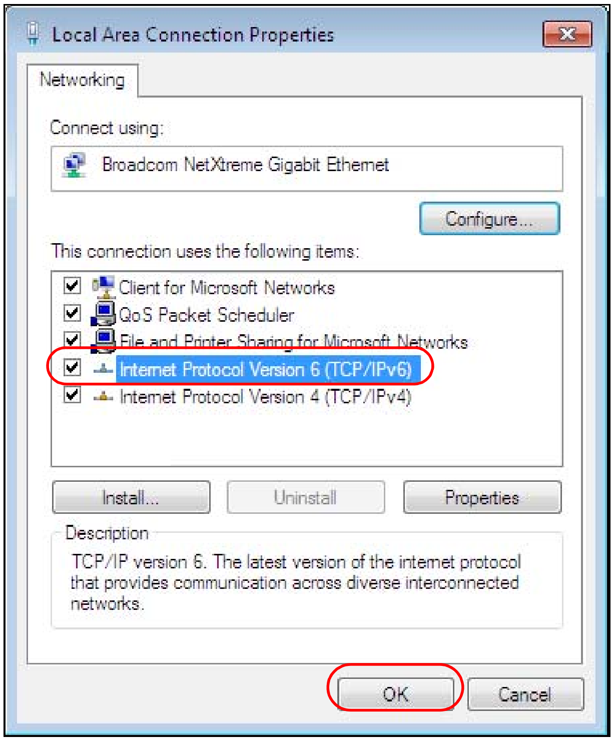
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.


Local Area Connection Properties
Networking
Connect using:
Broadcom NetXtreme Gigabit Ethernet
Configure...
This connection uses the following items:
Install...
Uninstall
Properties
Description
OK
Cancel

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 146 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL’s Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks’ messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.

Table 146 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SMTP	TCP	587	This is a more secure version of SMTP that authenticates sender from out of network mailservers.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 146 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

G

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- This IEEE 802.11 b/g/n product can only use channels 1 to 11 (frequency bands 2.412 to 2.462) in the United States of America.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用
者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class [*] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [*] est conforme à la norme NMB-003 du Canada.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 2012/19/UE (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 2012/19/UE (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2012/19/UE.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2012/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2012/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 2012/19/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 2012/19/UE.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2012/19/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2012/19/EC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2012/19/UE.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2012/19/UE del Parlamento eruopeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE).
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 2012/19/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2012/19/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2012/19/UE.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2012/19/UE.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2012/19/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2012/19/UE.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2012/19/UE.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2012/19/UE.

[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2012/19/UE.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2012/19/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2012/19/UE.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2012/19/ЕC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2012/19/UE.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2012/19/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2012/19/UE.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 2012/19/UE) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 2012/19/UE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 2012/19/UE) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2012/19/UE has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index