VFG6005 Series

VPN Firewall Gateway

User's Guide

IP Address	http://192.168.10.1
Login	admin
Password	1234

Firmware Version 2.07
Edition 1, 5/2011
www.us.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the VFG6005 Series using the Web Configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Supporting Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.us.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address. Thank you!

SUPPORT E-MAIL	WEB SITE
techwriter@zyxel.com	www.zyxel.com

Customer Support

Please have the following information ready when you contact Customer Support:

- Product model and serial number
- Warranty information
- Date that you received or purchased your device
- Brief description of the problem including any steps that you have taken before contacting the ZyXEL Customer Support representative

Support Email	support@zyxel.com
Toll-Free	1-800-978-7222
Website	www.us.zyxel.com
Postal mail	ZyXEL Communications Inc. 1130 N. Miller Street, Anaheim, CA 92806-2001 U.S.A.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The VFG6005 series may be referred to as the "VFG", the "device", the "product" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Admin > Log** means you first click **Admin** in the navigation panel, then the **Log** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The VFG icon is not an exact representation of your device.

VFG6005 Series 	Computer 	Notebook computer 
Server 	Modem 	Firewall 
Telephone 	Switch 	Router 

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 power outlet.
- 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.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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. 

Table of Contents

CHAPTER1 INTRODUCTION

ZyXEL's VFG6005 Series VPN Firewall Gateway is designed for small/home offices that need an entry level Firewall to protect their data from Internet threats and exploits. VPN support allows for a secure method to access the Local Area Network remotely on your laptop while on the road or to another office using a site-to-site tunnel to another VFG6005 series VPN Firewall Gateway. You can also create a secure mobile broadband hotspot anytime anywhere for a group of users and devices to share by using a Mobile Cellular USB modem. Since the mobile broadband is shared, this allows you to share the cost among several devices instead of being tied to a single PC or laptop. Furthermore, ZyXEL's VFG6005 Series VPN Firewall Gateway also supports 802.11n technology (VFG6005N), so you can enjoy the fastest and farthest wireless coverage!

1.1 BENEFITS

- **True Mobile Broadband Sharing (Supports xDSL/cable modem and Mobile Cellular + 802.11n)**
  ZyXEL's VFG6005 Series VPN Firewall Gateway supports multiple broadband technologies, including xDSL/cable modem and Mobile Cellular USB modem. You can create a mobile broadband hotspot using a USB modem or switch to a fixed line connection using an xDSL/cable modem. It also supports the latest 802.11n wireless technology (VFG6005N), offering a true mobile broadband sharing solution!

- **Complete Mobile Cellular USB Modem Support**
  ZyXEL's VFG6005 Series VPN Firewall Gateway provides support for most major Mobile Cellular USB modems. Simply use your existing USB modem and service provider to create a mobile broadband sharing environment. (Find our compatibility list here: http://www.us.zyxel.com/vfg)

- **Energy Saving**
  With a low power consumption SoC (System on Chip) solution, ZyXEL's VFG6005 Series VPN Firewall Gateway provides lower power consumption characteristics which saves not only energy, but also our environment.

- **Session Manager**
  ZyXEL's VFG6005 Series VPN Firewall Gateway supports fast recycling sessions in order to guarantee a stable network connection and to accommodate more users/applications in the network.

- **Bandwidth Management**
  ZyXEL's VFG6005 Series VPN Firewall Gateway is able to automatically monitor your bandwidth usage, prioritize traffic, and allocate bandwidth to all applications and users. At the same time, it also is able to provide users with the freedom to customize their bandwidth allocation to meet their desired special requirements, granting a smooth and efficient network sharing system no matter the circumstances or usage scenario.

- **Throughput and Session Monitoring**
  Providing Throughput and Session MRTG graphs within the Graphical User Interface, this allows users to monitor

bandwidth usage without difficulty and manage the network with total convenience and ease.

- **Dual WAN Failover**

  ZyXEL's VFG6005 Series VPN Firewall Gateway supports failover functions between fixed line (xDSL/cable modem) and 3G, offering non-stop network connectivity. (Does not do load sharing on both connections at the same time).

- **PPTP and IPsec VPN Server**

  PPTP VPN support provides a secured data connection for use with Window's built in VPN Client, Android or iPhone smartphones or other legacy VPN Clients. IPSec VPN support provides enterprise level data security to full featured IPSec VPN Clients or other VPN gateways. In either case, ZyXEL's VFG6005 Series VPN Firewall Gateway has your VPN support covered.

1.2 PACKAGE CONTENT

- **One ZyXEL VFG6005/VFG6005N Series VPN Firewall Gateway**
- **One User Manual CD**
- **One Quick Installation Guide**
- **One Power Adaptor**
- **One Ethernet Network Cable**
- **One USB extension cable**
- **Two Detachable Dipole Antennas (VFG6005N only)**

CHAPTER2 HARDWARE INSTALLATION

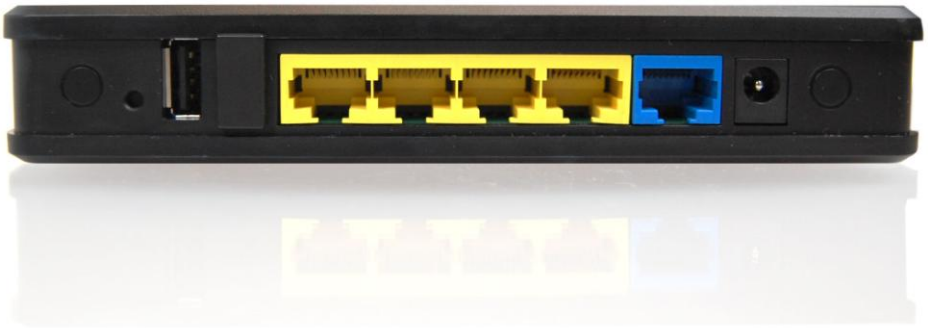
2.1 PANEL LAYOUT

2.1.1 Front LEDs (left to right)

LED	Function	Color	Status	Description
Power	Power Indication	Green	On	Power is on and system is ready.
			Off	Power is off
			Blinking	System is booting up.
WLAN	Wireless Activity	Green	On	Wireless connection is enabled
			Off	Wireless connection is disabled
		Red	On	ZyXEL VFG6005 Series VPN Firewall Gateway is faulty; please contact our customer service team. (contact info at the end of this document)
WAN	WAN Activity	Green	On	The Ethernet WAN port is connected
			Blinking	Data is being transmitted via the WAN port
			Off	Ethernet/Mobile WAN is disconnected.
		Orange	On	The Mobile WAN is connected
LAN(1, 2, 3, 4)	LAN Activity	Green	On	The Ethernet LAN port is connected
			Off	The Ethernet LAN port is not connected

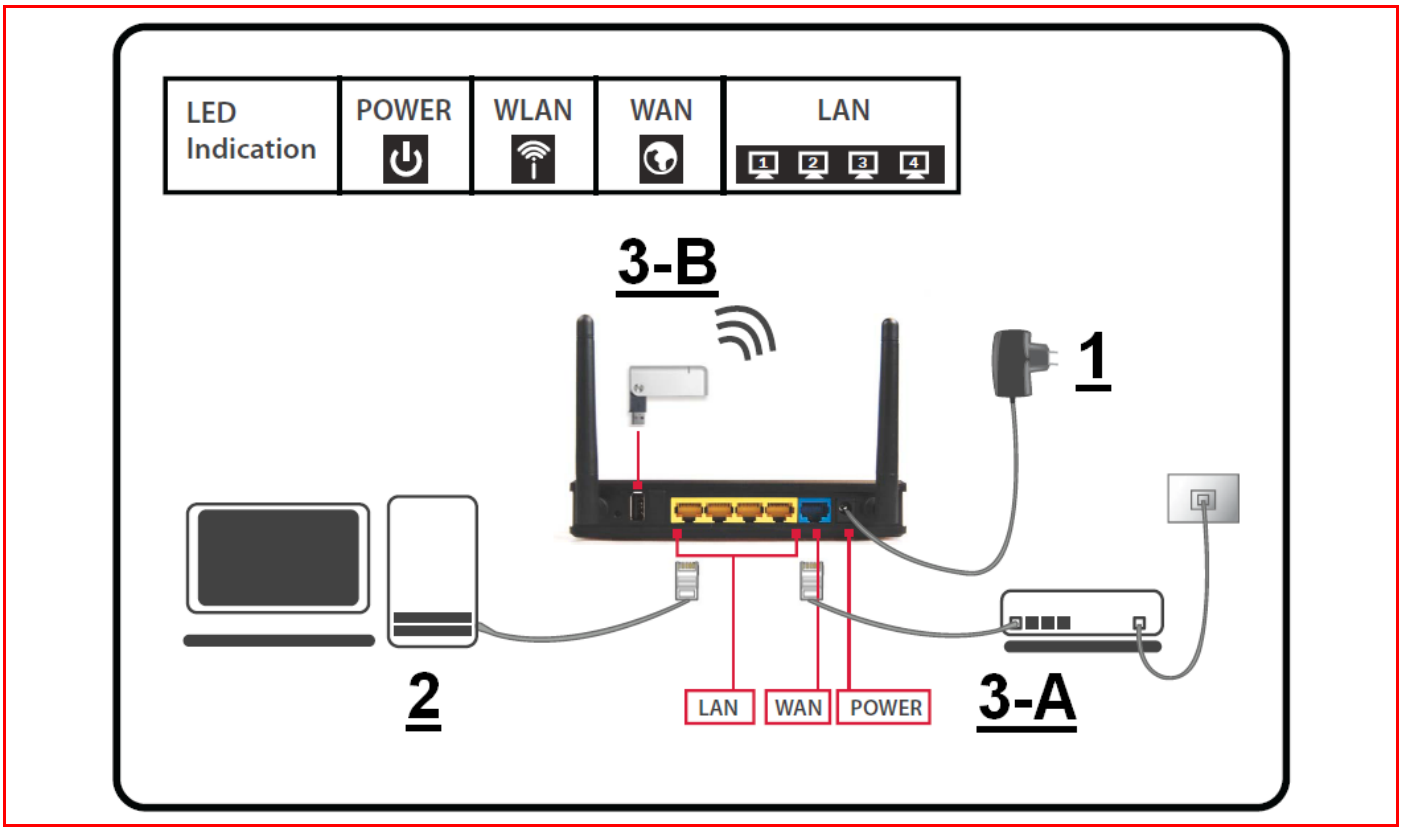
1 2 3 4			Blinking	Data is being transmitted via the LAN port

2.1.2 Rear Panel (left to right)



Ports	Description
Reset	When the status LED turns green without blinking, please press the Reset button for 3 seconds. The ZyXEL VFG6005 Series VPN Firewall Gateway will restart automatically and reset the settings to factory default.
USB	The port for connecting your 3G USB adapter. Please use USB port 1 as indicated on the top cover. USB port 2 is not used.
LAN (yellow)	The ports for connecting your computers, printer or other devices for making a wired connection.
WAN (blue)	The port for connecting your DSL or Cable Modem.
Power	Power inlet.

2.2 PROCEDURE FOR HARDWARE INSTALLATION



2.2.1 Power On

Take the provided power adapter. Plug one end into The ZyXEL VFG6005 Series DC power port and the other end into a power outlet. The ZyXEL VFG6005 Series VPN Firewall Gateway POWER LED will blink during the boot up phase and be ready when its POWER LED is solid.

2.2.2 Setup LAN Connection

Take an Ethernet cable. Plug one end of the cable into your computer's network port and the other end into one of The ZyXEL VFG6005 Series VPN Firewall Gateway's LAN ports (yellow).

2.2.3 Setup WAN Connection

Choose how to connect the ZyXEL VFG6005 Series VPN Firewall Gateway to the Internet.

A: Connecting via xDSL or cable modem: take an Ethernet cable and plug one end of the cable into one of your modem's LAN ports and the other end into the WAN port (blue).

B: Connecting via 3G: please plug the 3G USB modem into USB port 1.

CHAPTER3 NETWORK SETTINGS FOR YOUR PC

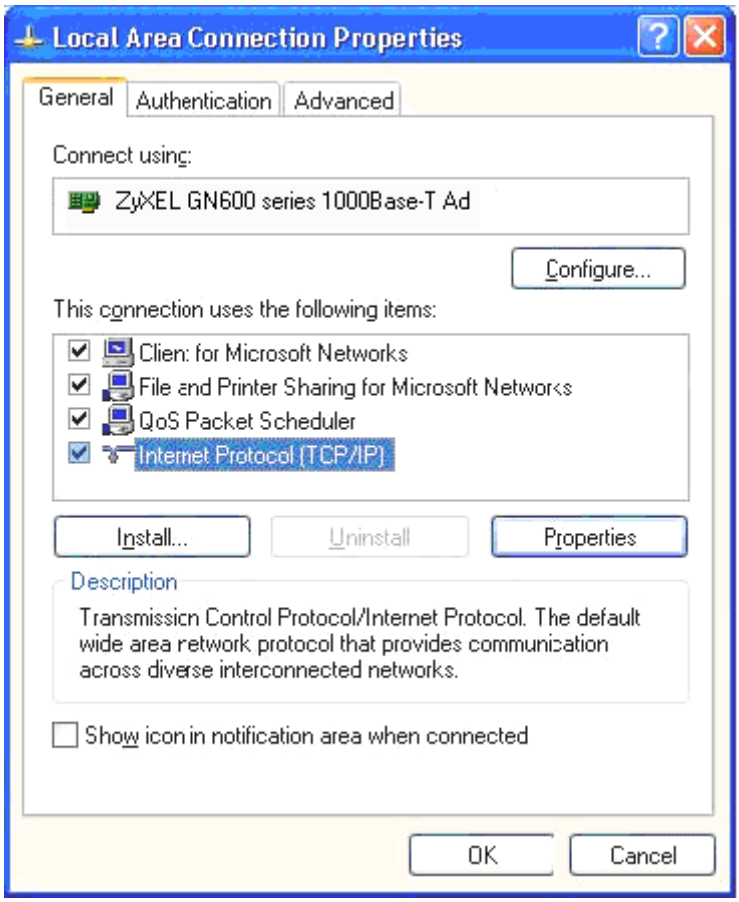
Before using the ZyXEL VFG6005 Series VPN Firewall Gateway, you have to configure your network settings in your computer. You can either use DHCP or Static IP for your TCP/IP Settings.

* DHCP is recommended due to its relative ease in configuration.

3.1 FOR WINDOWS XP USERS

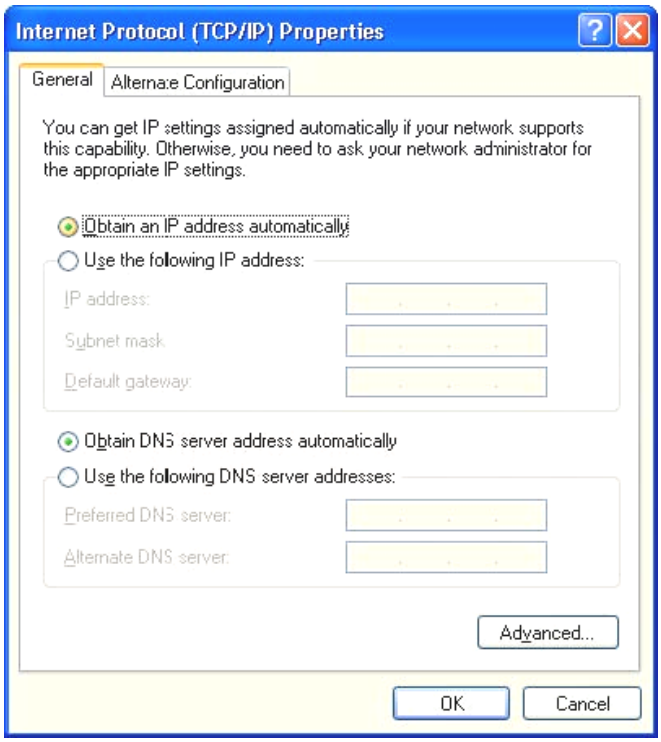
1. Select Start > Settings > Network Connections

2. Click on Local Area Connection and choose Properties. You will now see the following screen.



3. Select Internet Protocol (TCP/IP) for your network card.

4. Click on Properties. You will see the following screen.



5. Enable DHCP or Static IP:

- **To use DHCP**

Select Obtain an IP Address automatically and Obtain DNS server address automatically.

Then click OK. The ZyXEL VFG6005 Series VPN Firewall Gateway will now assign an IP address to your computer.

- **To use Static IP**

Select Use the following IP address and enter the followings.

IP address: 192.168.10.x (x could be from 2 ~ 254)

Subnet mask: 255.255.255.0

Default gateway: 192.168.10.1

Now select Use the following DNS server addresses and enter the following.

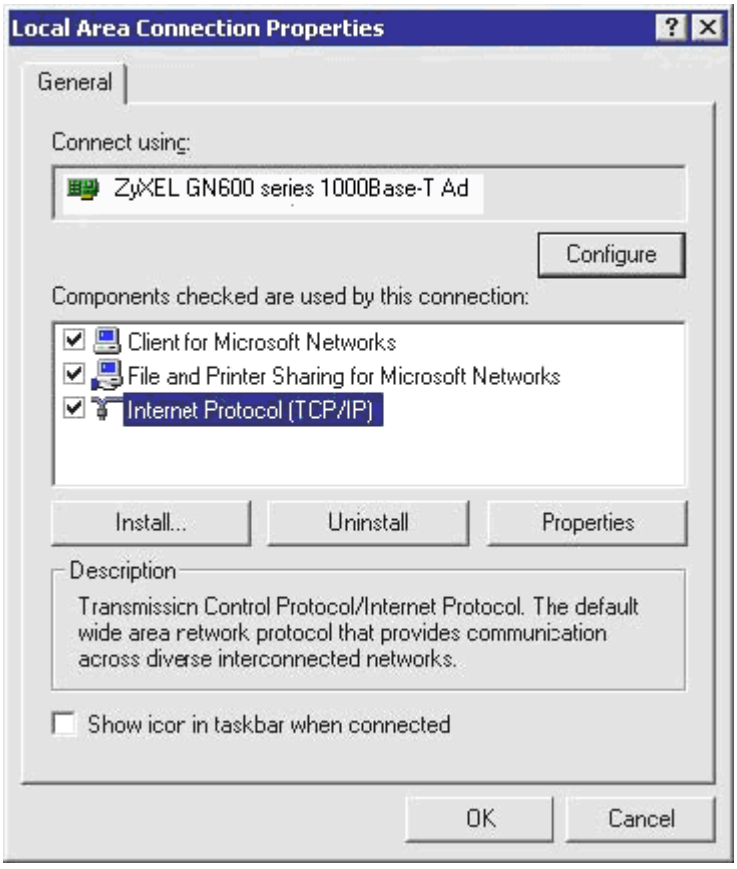
Preferred DNS server: 192.168.10.1. Then click OK.

6. You have now finished the network settings for your computer. Please go to Chapter 4 to continue.

3.2 FOR WINDOWS 2000 USERS

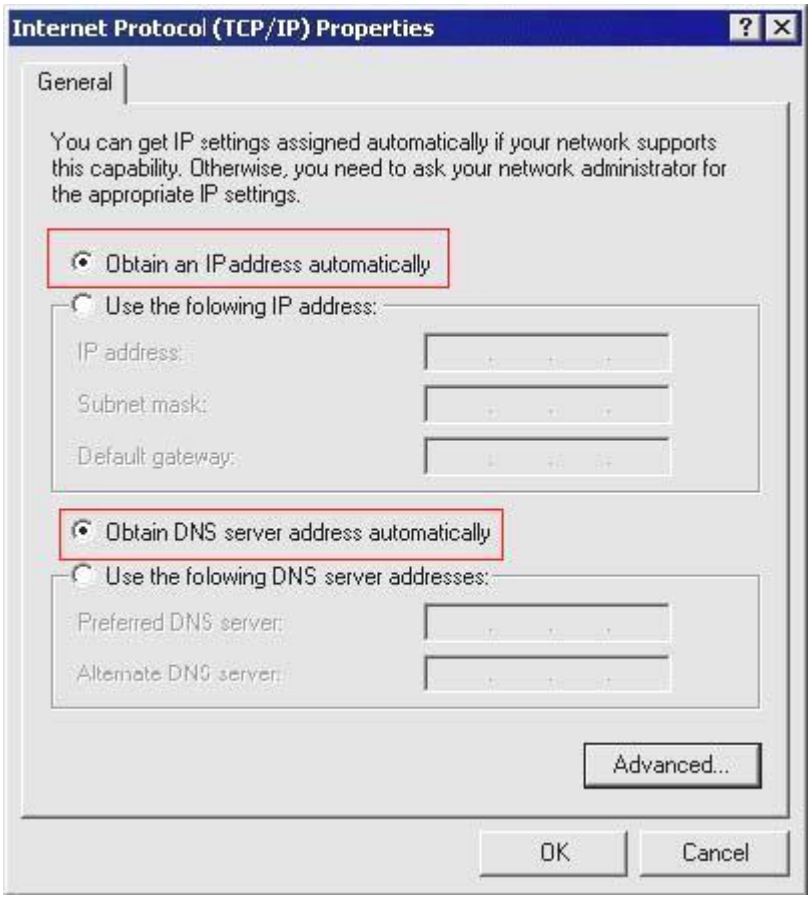
7. Select Start > Settings > Network and Dial-up Connection

8. Right click on the Local Area Connection and select Properties. You will see the following screen.



9. Select the Internet Protocol (TCP/IP) for your network card.

10. Click on Properties. You will see the following screen.



11. Enable DHCP or Static IP:

- **To use <u>DHCP</u>**

Select Obtain an IP Address automatically and Obtain DNS server address automatically.

Then click OK. The ZyXEL VFG6005 Series VPN Firewall Gateway will now assign an IP address to your computer.

- **To use <u>Static IP</u>**

Select Use the following IP address and enter the followings.

IP address: 192.168.10.x (x could be from 2 ~ 254)

Subnet mask: 255.255.255.0

Default gateway: 192.168.10.1

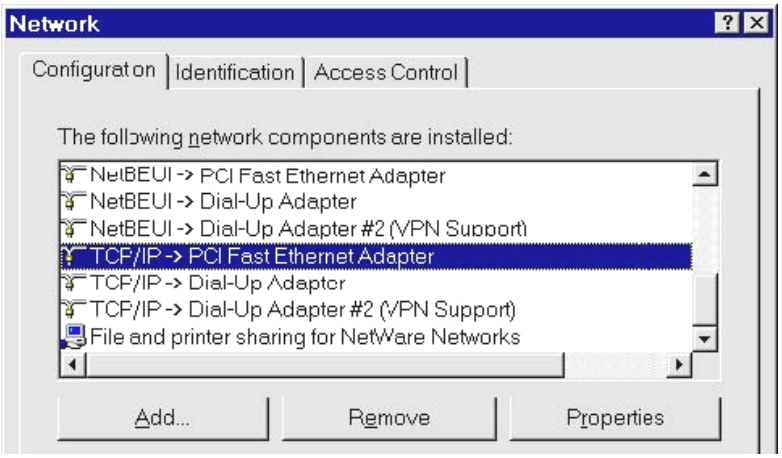
Now select Use the following DNS server addresses and enter the following. Preferred DNS server: 192.168.10.1

Then click OK.

12. You have now finished the network settings of your computer. Please go to Chapter 4 to continue.

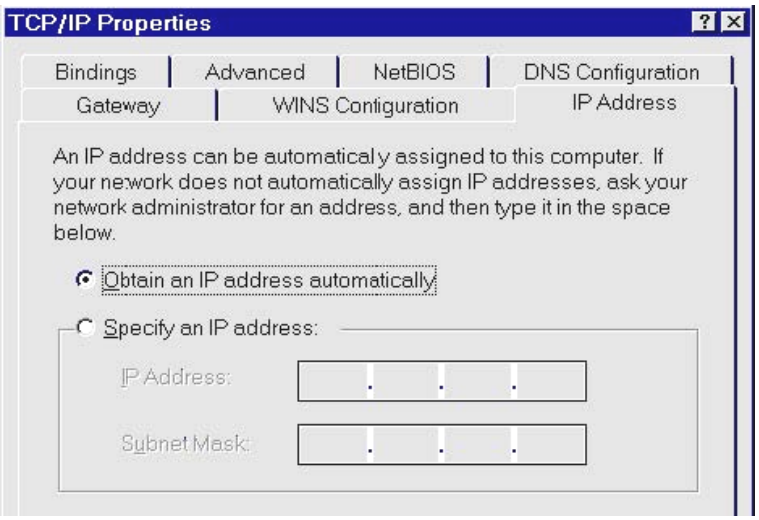
3.3 FOR WINDOWS 98/ME USERS

13. Select Start > Settings > Network. You will see the following screen.



14. Select TCP/IP -> PCI Fast Ethernet Adapter for your network card.

15. Click on Properties. You will now the following screen.



16. Enable DHCP or Static IP:

- **To use DHCP**

Select Obtain an IP Address automatically.

Then click OK. The ZyXEL VFG6005 Series VPN Firewall Gateway will now assign an IP address to your computer.

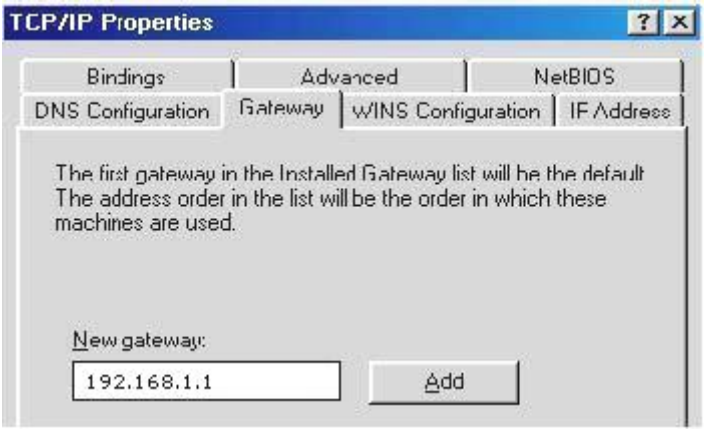
- **To use <u>Static IP</u>**

Select Specify an IP address and enter the followings.

IP address: 192.168.10.x (x could be from 2 ~ 254)

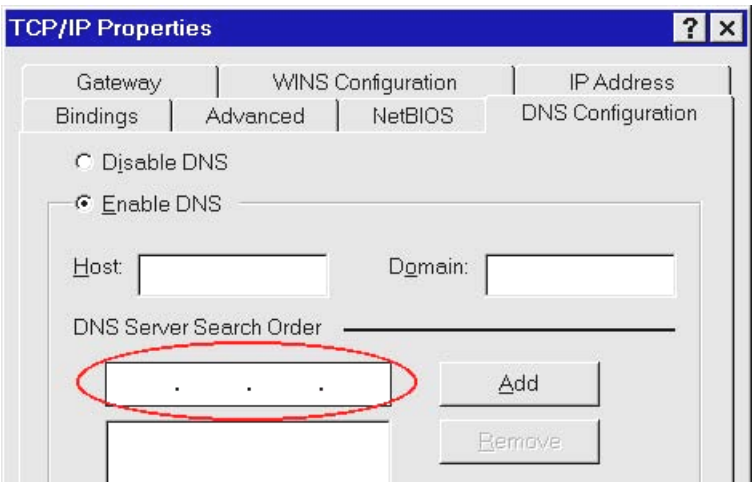
Subnet mask: 255.255.255.0

Now click on Gateway tab. You will see the following screen.



Enter 192.168.10.1 in *New Gateway,* and click *Add*.

Now click on the DNS Configuration tab. You will see the following screen.



Enter 192.168.10.1 in *DNS Server Search Order* and click *Add*.

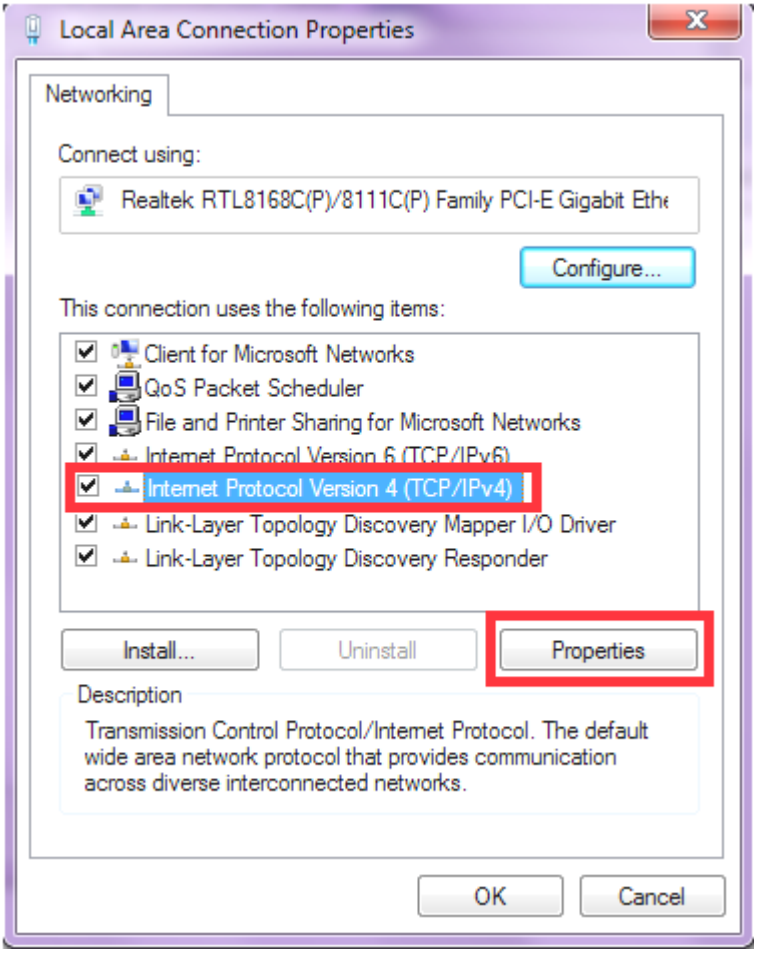
Then click *OK*.

17. You have now finished the network settings of your computer. Please go to Chapter 4 to continue.

3.4 FOR WINDOWS 7 USERS

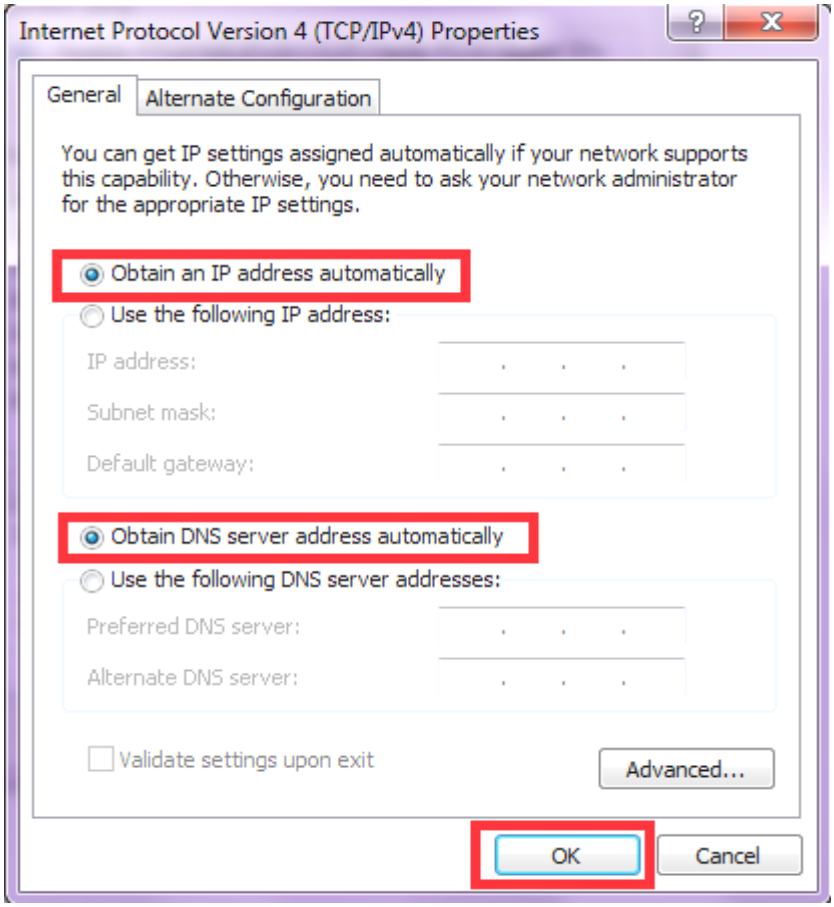
18. Select Start > Control Panel > Network and Internet> Network and Sharing Center >Change Adapter Settings

19. Click on Local Area Connection and choose Properties. You will now see the following screen.



20. Select Internet Protocol (TCP/IP) for your network card.

21. Click on Properties. You will see the following screen.



22. Enable DHCP or Static IP:

CHAPTER4 ACCESSING THE GATEWAY

For Windows XP/2000 users, your computer should have obtained an IP address after configuring the network settings on your computer. Now you need to configure your The ZyXEL VFG6005 Series VPN Firewall Gateway.

4.1 START-UP AND LOG-IN

Open your WEB browser. In the address box, enter [.HTTP://192.168.10.1]

When you successfully connect to the configuration interface for the ZyXEL VFG6005 Series VPN Firewall Gateway, the login screen will pop up. Enter your username as [admin] and your password as [1234]. You will now see the Router>Status page of The ZyXEL VFG6005 Series VPN Firewall Gateway. For initial Router Setup, **please consult the Quick Start Guide**.

CHAPTER5 BASIC SETTINGS

5.1 WAN SETUP

23. Click on [Setup] - [WAN] tab. You will see the following screen.

Setup - WAN

Ethernet WAN

WAN	(•) Enable ( ) Disable
Connection Type	DHCP
Host Name	
MTU	1500 Bytes

MAC Address Clone - Ethernet WAN

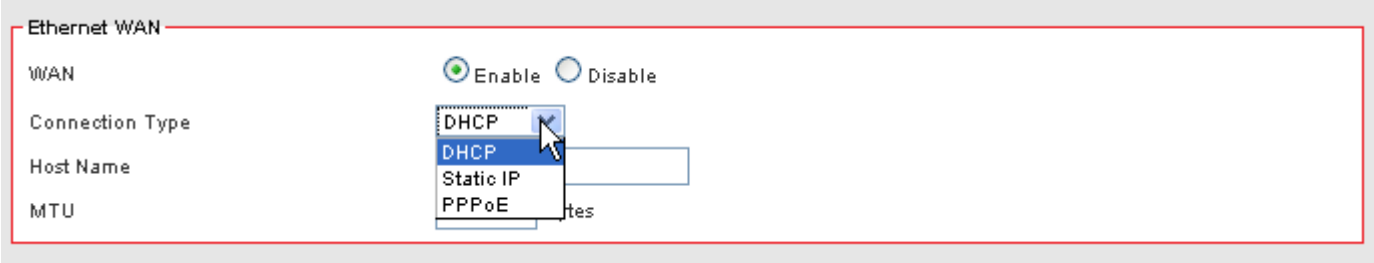
Clone WAN MAC	( ) Enable (•) Disable
MAC Address	Get My MAC

Mobile WAN

WAN	(•) Enable ( ) Disable
Connection Type	3G Mobile Internet
Modem Brand	Sierra
Modem Model	AirCard 598U
APN Type	(•) Service Provider ( ) Manual
Service Provider	Sprint
Access Point Name (APN)	
Personal Identification Number (PIN)	
Authentication	CHAP (Auto)
User Name	
Password	
Dial Number	#777
Connection Mode	Auto
PPP Connection Type	(•) Keep Alive ( ) On Demand

24. WAN Settings:

The ZyXEL VFG6005 Series VPN Firewall Gateway supports Ethernet WAN and Mobile WAN. Ethernet WAN has three connection types: DHCP, Static and PPPoE. Please ensure which connection type should be used, and select your internet connection type from the pull-down menu.

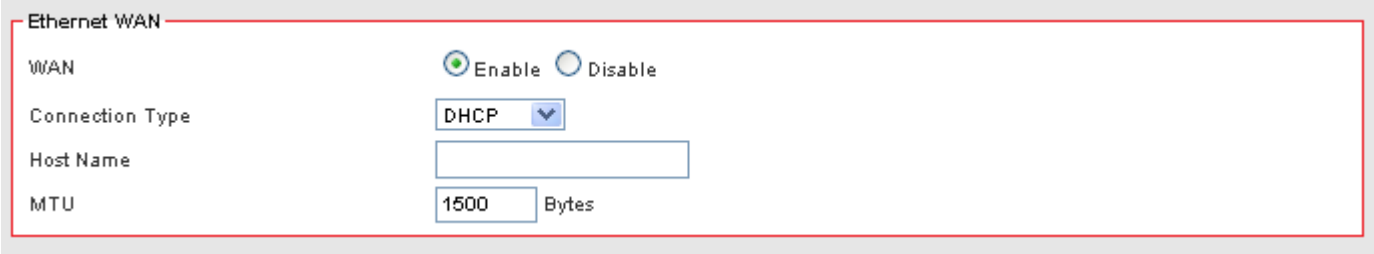


Whatever WAN connection type you have chosen, The ZyXEL VFG6005 Series VPN Firewall Gateway will get a WAN IP and this IP will be shown in the Router/Status page as below.

If “Not Connected” shows up in the setting, you should check the WAN settings again to get correct connection

5.1.1 DHCP (automatic IP address assignment)

The IP address is automatically assigned to you by your ISP. You will see the following screen when you choose DHCP.

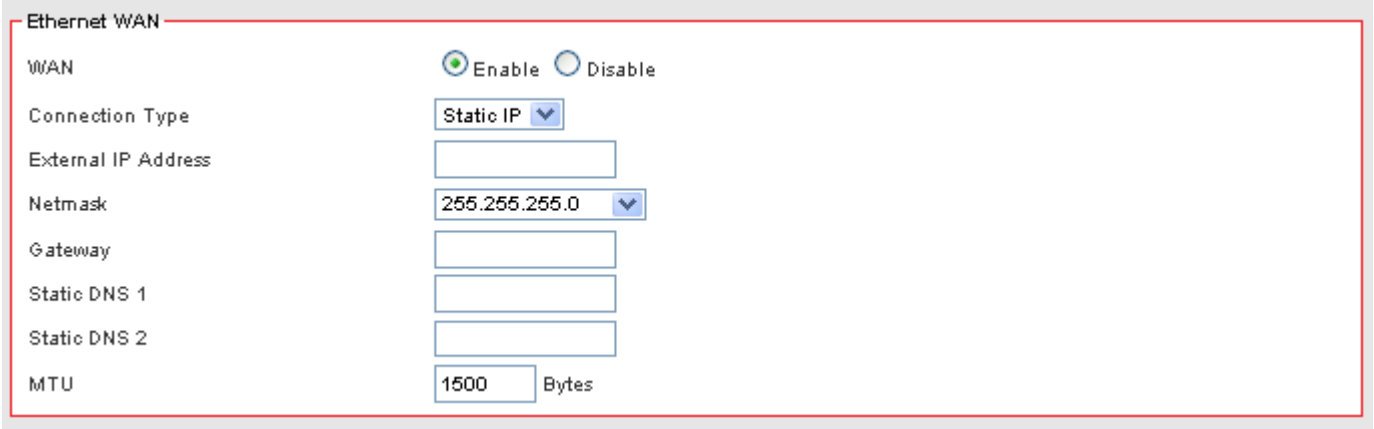


WAN	Select Enable/Disable to enable/disable WAN
Connection Type	DHCP
Host Name	Some ISP and DHCP servers ask for the Host Name of the DHCP client before assigning an IP address. In this case, please key in your Host Name.
MTU	Maximum Transmission Unit

5.1.2 Static (Fixed IP address assignment)

The IP address, subnet mask, gateway, and DNS server are provided by your ISP.

Please enter the information accordingly.

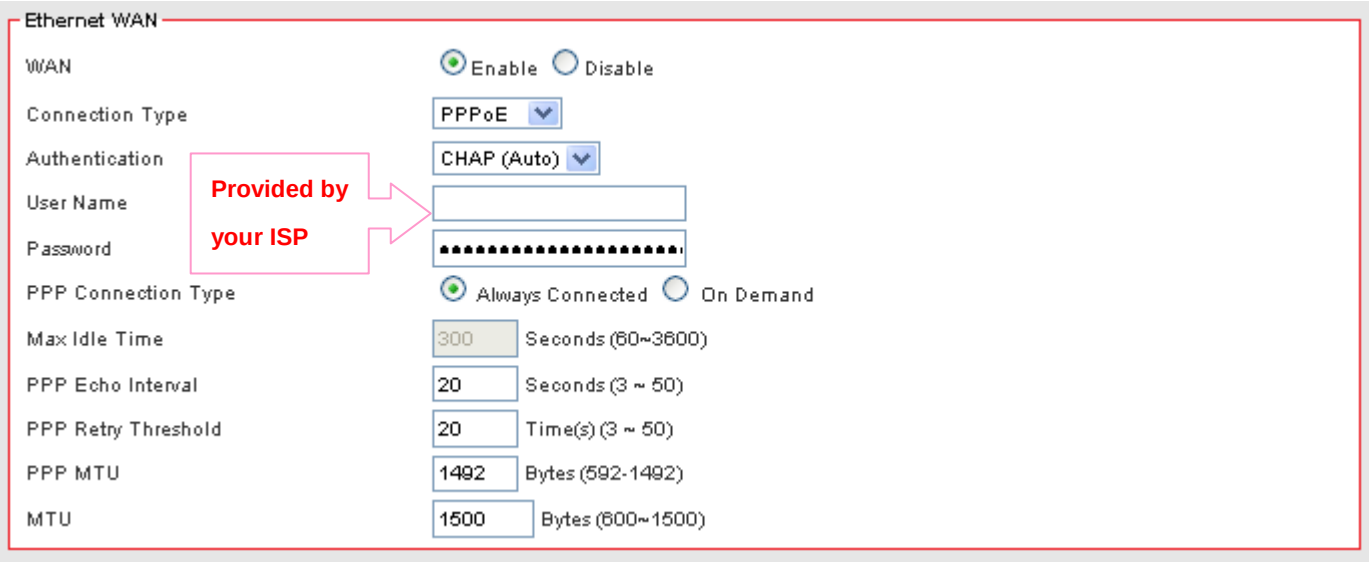


WAN	Select Enable / Disable to enable/disable WAN.
Connection Type	Static IP
External IP Address	The external IP addresses offered by the ISP.
Netmask	The netmask offered by the ISP.
Gateway	The gateway offered by the ISP.
Static DNS 1	The static DNS 1 offered by the ISP.

Static DNS 2	The static DNS 2 offered by the ISP.
MTU	Maximum Transmission Unit

5.1.3 PPPoE (connected by username/password)

If your ISP provides the username and password, please enter the information accordingly.

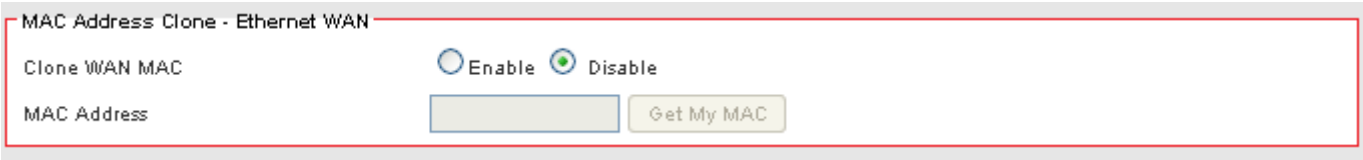


WAN	Select Enable/Disable to enable/disable WAN
Connection Type	PPPoE
Authentication	The authentication type CHAP or PAP offered by your ISP.
User Name	The user name offered by the ISP.
Password	The password offered by the ISP.
PPP Connection Type	Always Connected will maintain the PPPoE dial up connection. On Demand will connect only when there is traffic.
Max Idle Time	PPPoE On Demand will only be activated when there is traffic. When there is no traffic within the max idle time (default: 300 seconds), the PPPoE connection will be disconnected.
PPP Echo Interval	PPPoE echo will ensure whether the link is still up or not (default interval 20 seconds)
PPP Retry Threshold	When PPPoE echo retry exceeds PPPoE Retry Threshold (default 20 times), the dial up connection would be recognized as down.
PPP MTU	PPPoE maximum transmission unit: up to 1492 bytes (PPPoE's header is 8 bytes)(This value should be less than MTU value at least 8 bytes).
MTU	Physical Device Maximum Transmission Unit

5.1.4 Ethernet WAN MAC Address Clone

Some ISPs only allow a registered MAC address to access to the internet. To bypass the rule, you need to set up a cloned MAC address for The ZyXEL VFG6005 Series VPN Firewall Gateway using the pre-registered MAC address.

1. Click on [Setup] – [MAC Address Clone] tab. You will see the following screen.



2. Configure your MAC Clone for Ethernet WAN, Mobile WAN and LAN following the instructions below.

Clone WAN MAC	If your ISP only grants access to a fixed MAC address, please select Enable. If your ISP does not enforce access control, please select Disable.
MAC Address	If the PC you use to configure The ZyXEL VFG6005 Series VPN Firewall Gateway is the device which has the right MAC address to access the internet, press “Get My MAC” button. You can also type in the MAC Address which has been granted access by your ISP.

5.1.5 Mobile WAN (connected by information related to what your ISP needs)

Please enable and enter the APN, PIN code, user name, and password provided by your ISP. You may also choose from the list of profiles for well known ISP settings. (Please note that some information might not be needed.)

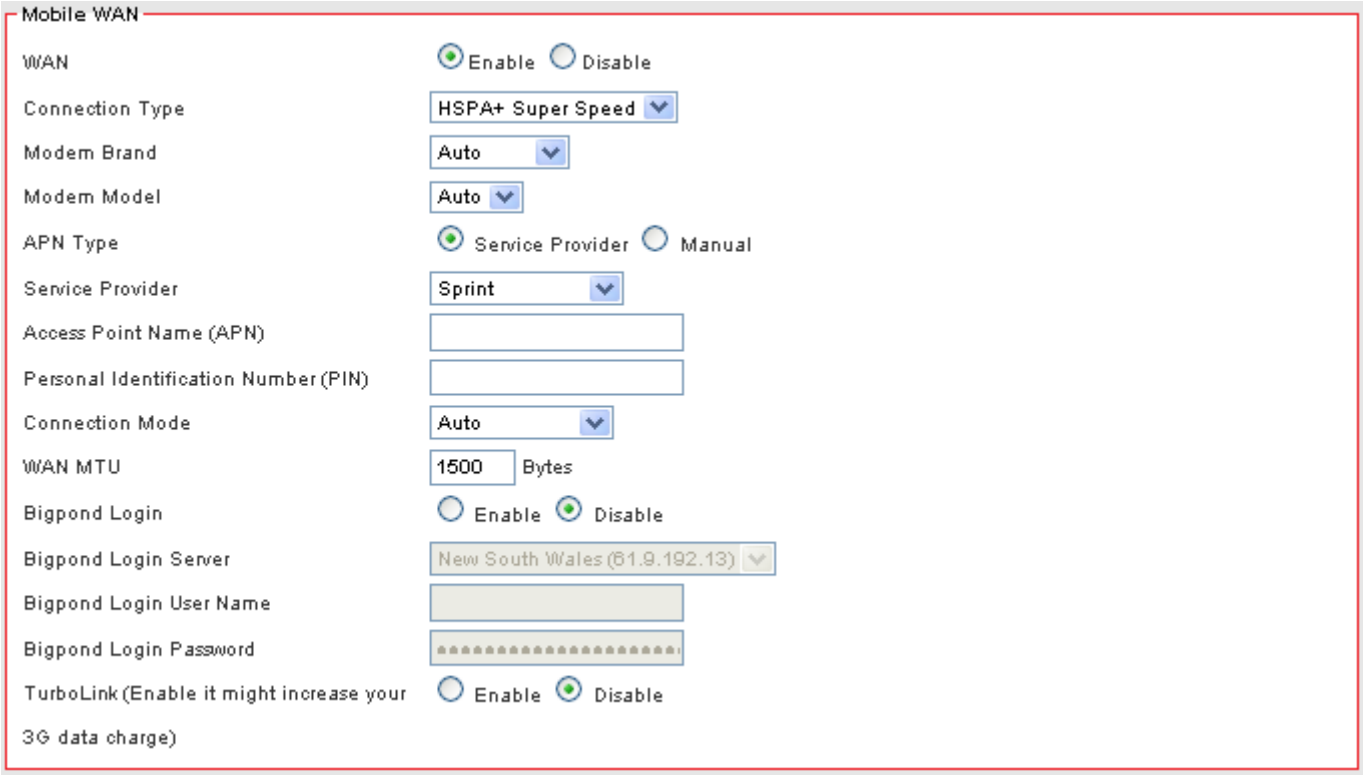
Mobile WAN

WAN	Enable Disable
Connection Type	3G Mobile Internet
Modem Brand	Auto
Modem Model	Auto
APN Type	Service Provider Manual
Service Provider	Sprint
Access Point Name (APN)	
Personal Identification Number (PIN)	
Authentication	CHAP (Auto)
User Name	
Password	
Dial Number	#777
Connection Mode	Auto
PPP Connection Type	Keep Alive On Demand
Max Idle Time	300 Seconds (60~3600)
PPP Echo Interval	20 Seconds (3 ~ 50)
PPP Retry Threshold	20 Time(s) (3 ~ 50)
Mobile WAN MTU	1492 Bytes (592-1492)
TurboLink (Enable it might increase your 3G data charge)	Enable Disable

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	Mobile WAN
Modem Brand	Select the modem brand you use. You can keep it as Auto for automatic detection.
Modem Model	Select the modem model you use. You can keep it as Auto for automatic detection.
APN Type	Select By Service Provider for specifying the ISP you use, or otherwise choose Custom to assign desired APN.
Service Provider	Select your service provider so the Access Point Name (APN) and the Dial Number will be automatically assigned.
Access Point Name (APN)	Enter APN string offered by the ISP if you select Custom for APN Type (keep it empty if your ISP doesn't need it).
Personal Identification Number (PIN)	Enter PIN code offered by the ISP (keep it empty if your ISP doesn't need it).
Authentication	Choose the authentication method CHAP, PAP or None.
User Name	The user name offered by the ISP (keep it empty if your ISP doesn't need it).
Password	The password offered by the ISP (keep it empty if your ISP doesn't need it).
Dial Number	Enter Dial Number offered by the ISP.
Connection Mode	Sets the desired connection mode and speed (HSDPA, UMTS, EDGE, GPRS).
PPP Connection Type	PPPoE Keep Alive will maintain the PPPoE dial up connection.
Max Idle Time	Set the max idle time before the mobile WAN is disconnected. (default interval 300 seconds)
PPP Echo Interval	PPPoE echo will ensure whether the link is still up or not (default interval 20 seconds)
PPP Retry Threshold	When PPPoE echo retry exceeds PPPoE Retry Threshold (default 20 times), the dial up connection would be recognized as down.
PPPoE MTU	PPPoE maximum transmission unit: up to 1492 bytes (PPPoE's header is 8 bytes).

5.1.6 HSPA+ Super Speed

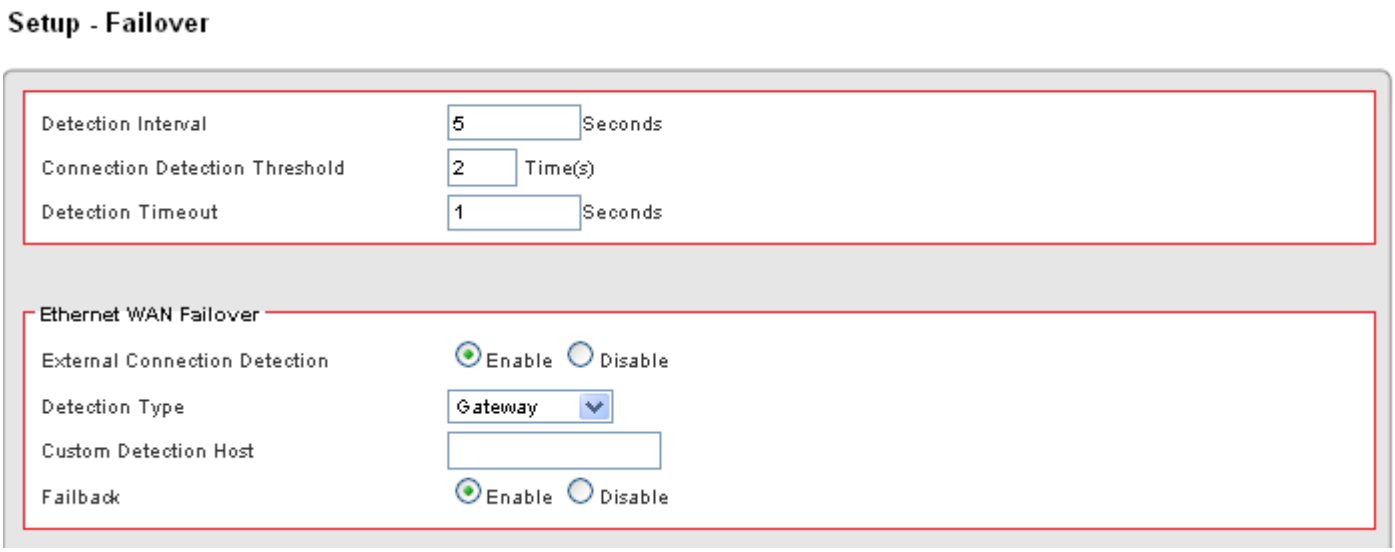
If you using HSPA+ super speed modem, please choose this WAN connection type. Please enable and enter the APN, PIN code, user name, and password provided by your ISP. You may also choose from the list of profiles for well known ISP settings. (Please note that some information might not be needed.)



WAN	Select Enable/Disable to enable/disable WAN
Connection Type	HSPA+ Super Speed
Modem Brand	Select the modem brand you use. You can keep it as Auto for automatic detection.
Modem Model	Select the modem model you use. You can keep it as Auto for automatic detection.
APN Type	Select By Service Provider for specifying the ISP you use, or otherwise choose Custom to assign desired APN.
Service Provider	Select your service provider and the Access Point Name (APN) will be automatically assigned.
Access Point Name (APN)	Select By Service Provider for specifying the ISP you use, or otherwise choose Custom to assign desired APN.
Personal Identification Number (PIN)	Please enter PIN code
Connection Mode	Select your connection mode. (AUTO mode recommended)
WAN MTU	Maximum transmission unit
Bigpond Login	If you are using “Bigpond” system, please enable this item
Bigpond Login Server	Please choose the Bigpond server.
Bigpond Login User Name	Please enter your User Name provided by Bigpond
Bigpond Login Password	Please enter your Password provided by Bigpond
TurboLink	Enable “TurboLink” to improve the connection speed and stability. (Please note that TurboLink function might increase your 3G data charge)

5.2 WAN DETECT

3. Click on [Setup] – [WAN Failover] tab. You will see the following screen.

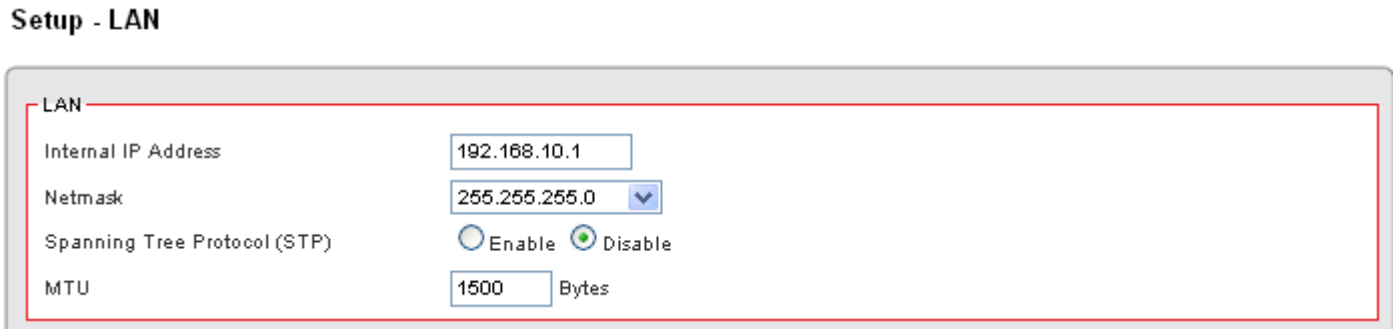


4. Configure the basic settings of WAN Failover following the instructions below.

Detection Interval	This is the interval which specifies how often the VFG6005 series will check the Ethernet WAN connection.
Connection Detection Threshold	The system will generate a PING packet to detect whether the Ethernet WAN connection is still connected. If the Host has not responded for this threshold value, the system is considered to be Ethernet WAN link down.
Detection Timeout	This is the timeout time before the connection ping is considered lost.
External Connection Detection	Select Enable/Disable to enable/disable connection detection. This is required for failover from Ethernet WAN to Mobile WAN.
Detection Type	Select Gateway or use your own custom Host IP. The VFG6005 series will check the connection to this IP periodically. If at any time the connection ping is lost for the threshold set, the VFG6005 series will switch WAN traffic from Ethernet WAN to Mobile WAN if available.
Custom Detection Host	Enter the IP address or domain name of the host to be detected.
Fallback	Enable this if you wish for the Mobile WAN connection to fall back to Ethernet WAN when it is available.

5.3 LAN SETUP

1. Click on [Setup] – [LAN] tab. You will see the following screen.



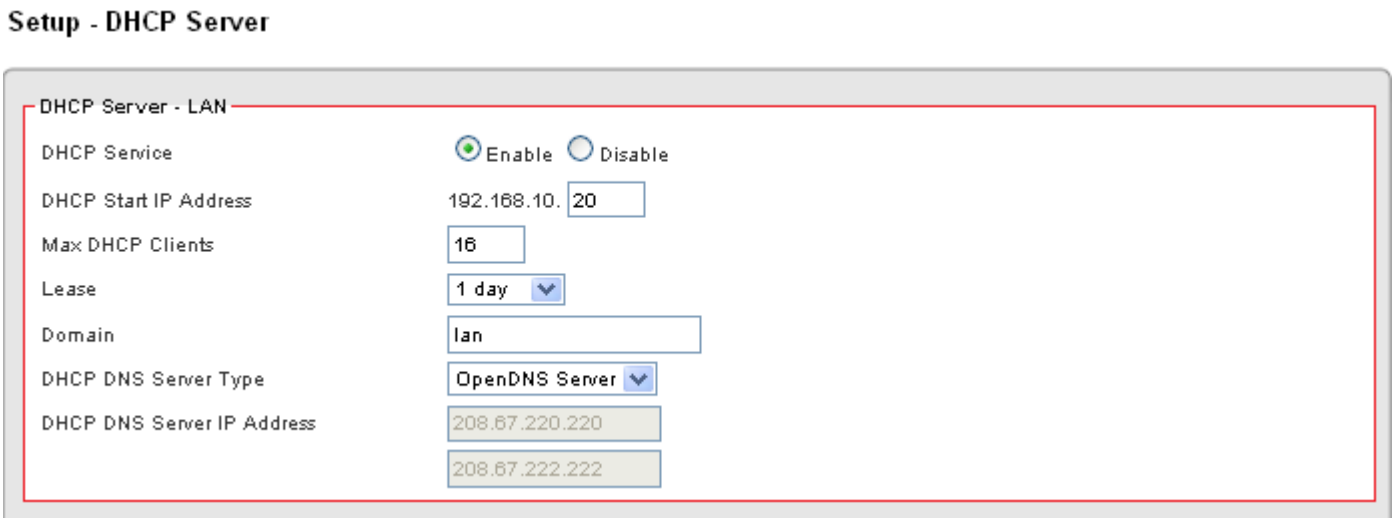
2. Configure your LAN following the instructions listed below.

Internal IP Address	Please key in Internal IP Address
Netmask	Select Netmask from the selection list.
Spanning Tree Protocol (STP)	Click Enable only if you will deploy your network in a ring topology. Other switches in the LAN must also support STP. (A cyclic topology will cause network breakdown with STP enabled.)
MTU	Maximum transmission unit: up to 1500 bytes.

5.4 DHCP SERVER SETUP

The ZyXEL VFG6005 Series VPN Firewall Gateway provides DHCP server service in order to offer IP addresses to the computers within a LAN.

1. Click on [Setup] – [DHCP Server] tab. You will see the following screen.



2. Configure your LAN following the instructions listed below.

DHCP Service	Select Enable/Disable to enable/disable DHCP Server.
DHCP Starting IP Address	The DHCP starting IP addresses offered by the DHCP Server.
Max DHCP Clients	The maximum number of the IP addresses supported by the DHCP server
Lease	Please choose lease time from the selection list. You can choose 1 Hour, 3 Hours, 6 Hours, 1 Day, 3 Days, or 7 Days.
Domain	Please enter the domain name.
DHCP DNS Server Type	Select OpenDNS Server if you have an OpenDNS account for content filtering. Otherwise choose ISP DNS Server to use your ISP's default server or Custom to enter your own IP address.
DHCP DNS Server IP Address	Enter Custom IP address for DNS here.

5.5 DDNS SETUP

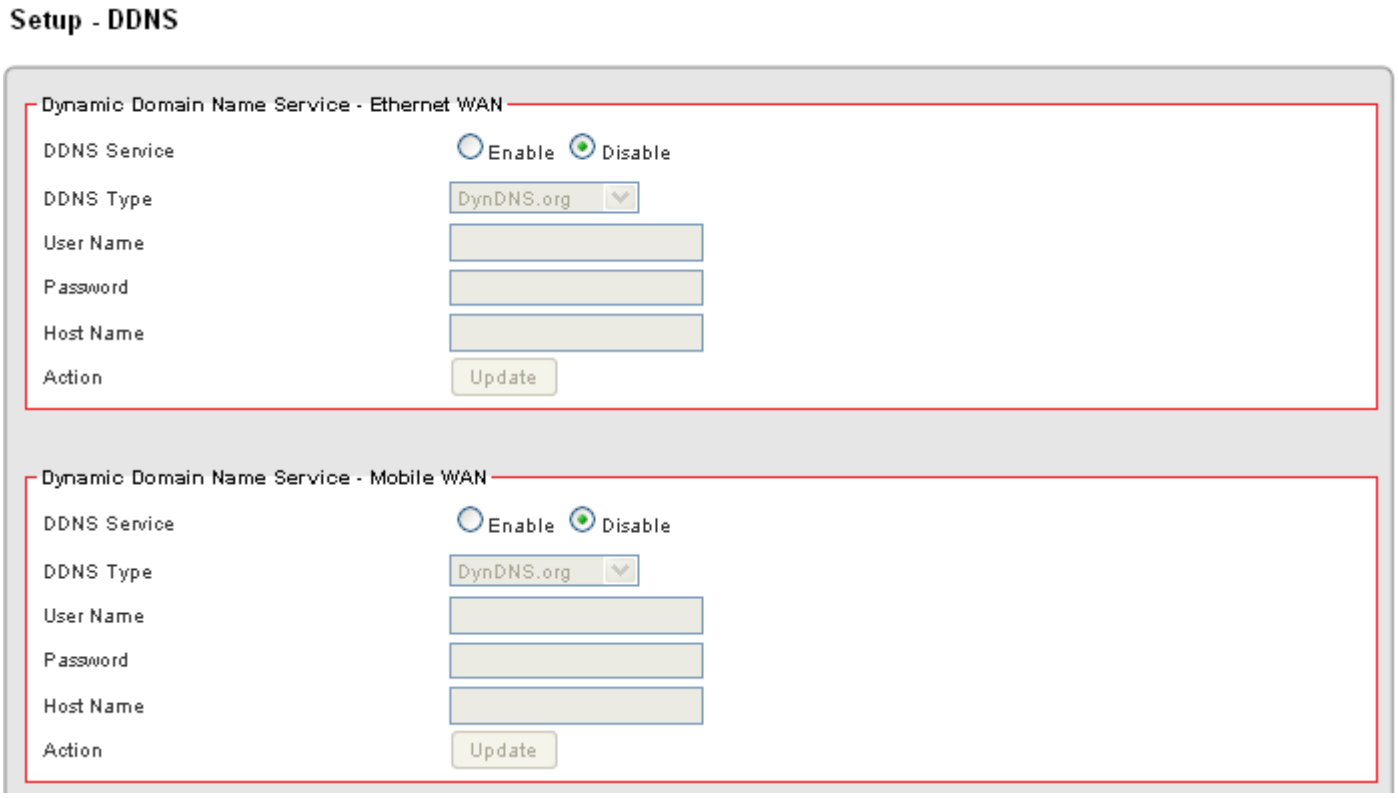
DDNS (Dynamic Domain Name Service) allows an “internet domain name” to be assigned to a computer/router which has a dynamic IP address. This makes it possible for other internet devices to connect to the computer/router without needing to trace the changing IP addresses themselves. To enable DDNS, you will first need to sign up for DDNS services from DynDNS.org, TZO.com or ZoneEdit.com.

DDNS is useful when combined with the virtual server feature. It allows other internet users to connect to your virtual server by using a domain name, rather than an IP address. The DDNS service helps users to locate the right IP address by the domain name.

For example, you wish to set up a personal web server. However, you obtain a different IP address from your ISP every time you connect to the internet. The dynamic IP address you have will cause difficulty for other internet users to find your web server. In this case, you will need to enable DDNS, so other users can connect to you through a fixed domain name to disregard the potential varying IP addresses behind the server.

1. Register with one of the DDNS providers (DynDNS.org, TZO.com or ZoneEdit.com) before you configure DDNS on the ZyXEL VFG6005 Series VPN Firewall Gateway.

2. Click on [Setup] – [DDNS] tab. You will see the following screen.



3. Configure your DDNS following the instructions listed below.

DDNS Service	Select Enable to enable DDNS service. Select Disable to disable DDNS service.
DDNS Type	Select the desired DDNS service provider from the list.
User Name	Enter your username
Password	Enter your password
Host Name	Apply for a domain name, and make sure it is allocated to you
Action	Press Update button to immediately update DDNS information.

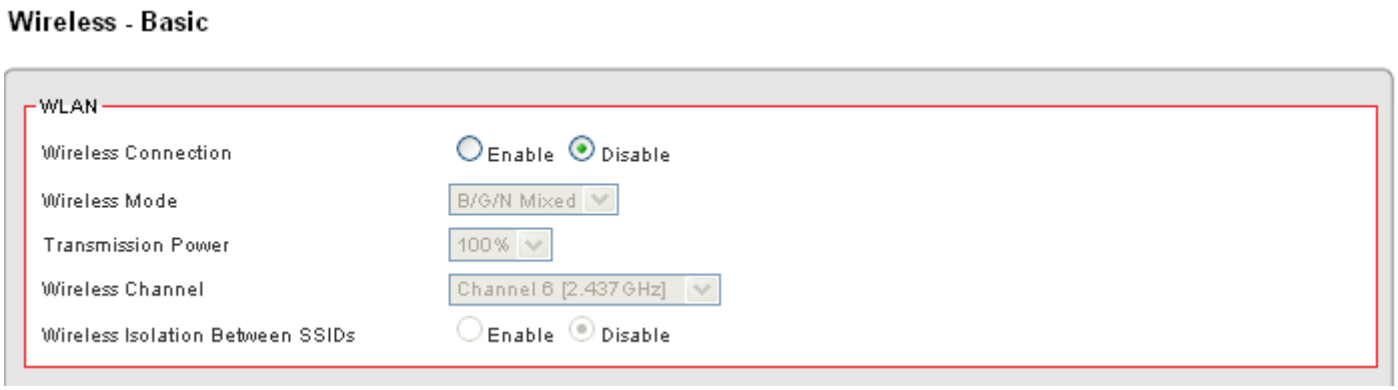
CHAPTER6 WIRELESS SETTINGS

6.1 BASIC SETUP

Multiple SSIDs allow the ability for separate security mode and key settings to be set by users for both convenience and increased protection. Users are able to configure their network devices to access the first SSID with the WPA2 PSK (Pre-Shared Key) and secret key, whilst share the second SSID with WEP and the periodically changed key for visitors. In addition, users are able to isolate these SSIDs to avoid malicious attacks and prevent certain access for visitors using the second SSID. This then provides users an extremely convenient approach to share the wireless access, provide access internet access for visitors, while possessing a strong security protection system at all times.

6.1.1 Settings

1. Click on [Wireless] – [Basic] tab. You will see the following screen.



2. Configure wireless settings following the instructions below.

Wireless Connection	Select Enable if you would like to turn on the wireless signal Select Disable if you would like to turn off the wireless signal.
Wireless Mode	Select the wireless mode for 802.11b/g/n or mixed use.
Transmission Power	Select the transmission power class from 10%, 25%, 50%, 75%, and 100%.
Wireless Channel	Select which channel to be located to.
Wireless Isolation Between SSIDs	Select Enable if you would like to block traffic from one SSID to another. Select Disable if you would like to allow traffic from one SSID to another.

6.1.2 SSID Settings

Users are able to configure each SSID with its own attributes. Further, various security modes are available based on the user's needs and preference: Disable, WEP, WPA Pre-Shared Key, WPA, WPA2 Pre-Shared Key, and WPA2. However, it is important to note that all devices under the wireless network must use the same security mode.

You can configure the security settings of your wireless network to suit your desired preference. Different methods will grant different levels of security. Using encryption - data packet is encrypted before transmission - can prevent data packets from being intruded on by un-trusted parties. However, please note that the higher the security level is, the lower the data throughput becomes.

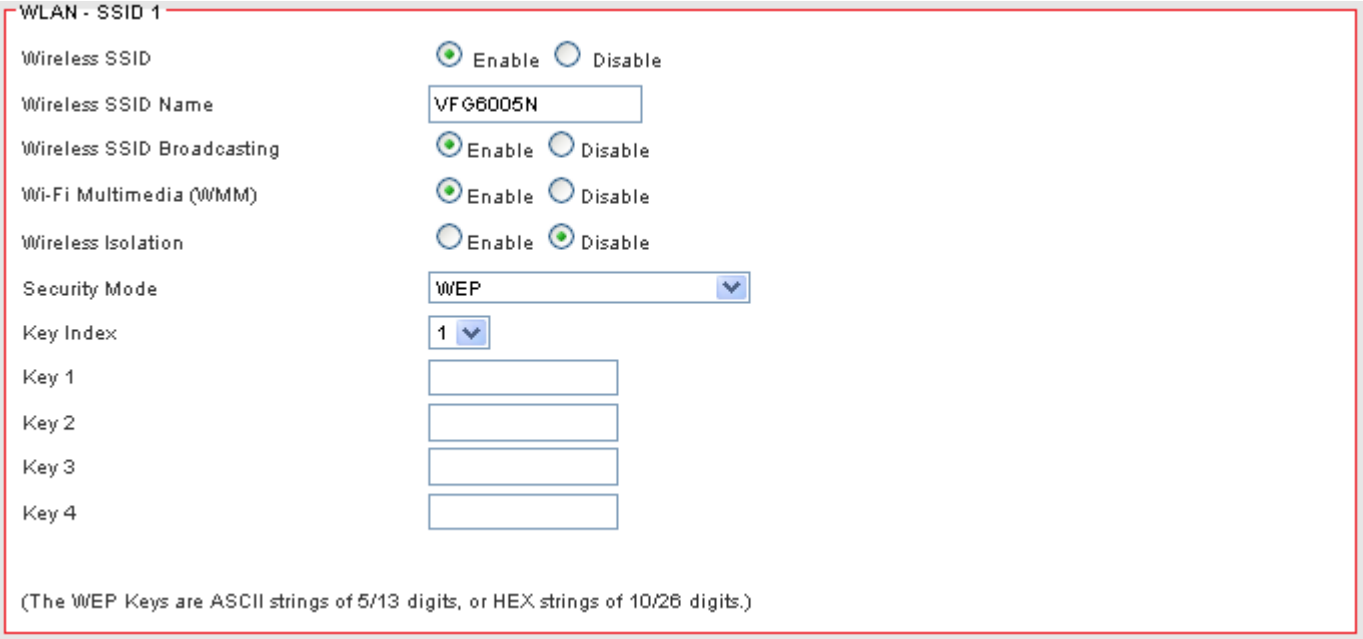
1. Click on [Wireless] – [Basic] tab. You will see the following screen.

2. Configure SSID settings following the instructions below.

Wireless SSID	Select Enable if you would like to turn on this SSID. Select Disable if you would like to turn off this SSID.
Wireless SSID Name	Enter the wireless station name you would like to have.
Wireless SSID Broadcasting	The ZyXEL VFG6005 Series VPN Firewall Gateway broadcasts SSID periodically. Select Enable to turn it on or Disable to turn it off. Enabling SSID Broadcasting brings convenience for users to find and connect The ZyXEL VFG6005 Series VPN Firewall Gateway. Disabling SSID broadcasting enhances the security by hiding SSID information.
Wi-Fi Multimedia (WMM)	Select Enable to prioritize different traffic types based on their characteristics. For example, VoIP or video traffic will have higher priorities over ordinary traffic.

Wireless Isolation	Select Enable if you would like to block traffic between other network devices connecting to this SSID. (recommended) Select Disable if you would like to allow traffic between other network devices connecting to this SSID.
Security Mode	Select WEP/WPA-PSK/WPA/WPA2-PSK/WPA2 for security mode. (WPA2-PSK recommended)

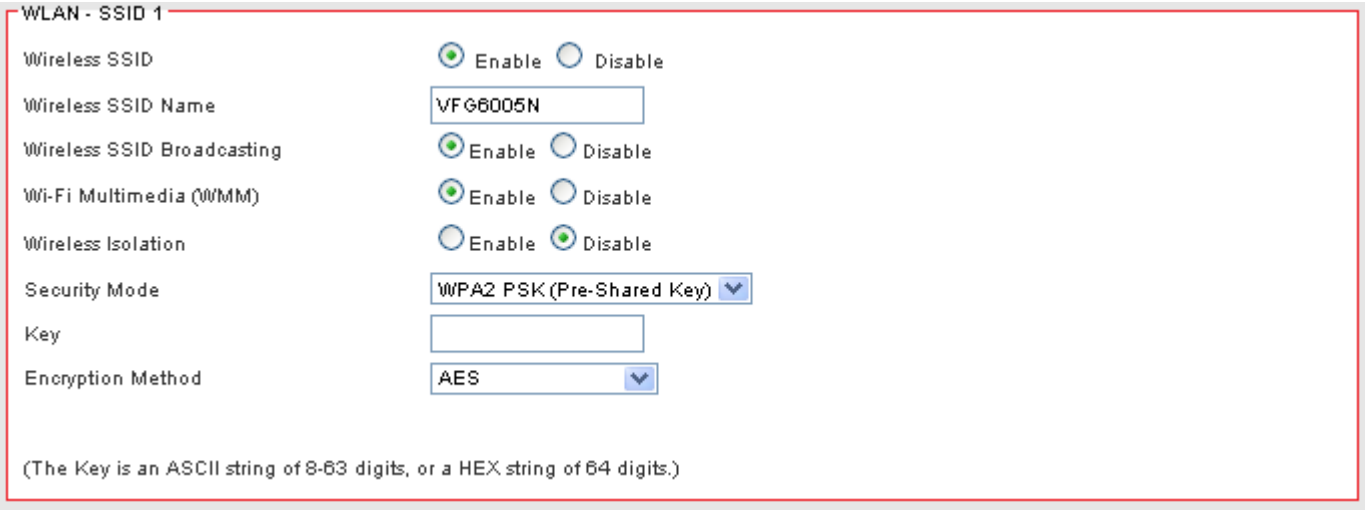
6.1.3 WEP



If WEP is selected, WEP index and keys should be set manually.

WEP Key Index	WEP Key Index indicates which WEP key is used for data encryption.
WEP Key (1~4)	64-bit WEP: type 10 hexadecimal digits or 5 ASCII characters 128-bit WEP: type 26 hexadecimal digits or 13 ASCII characters.

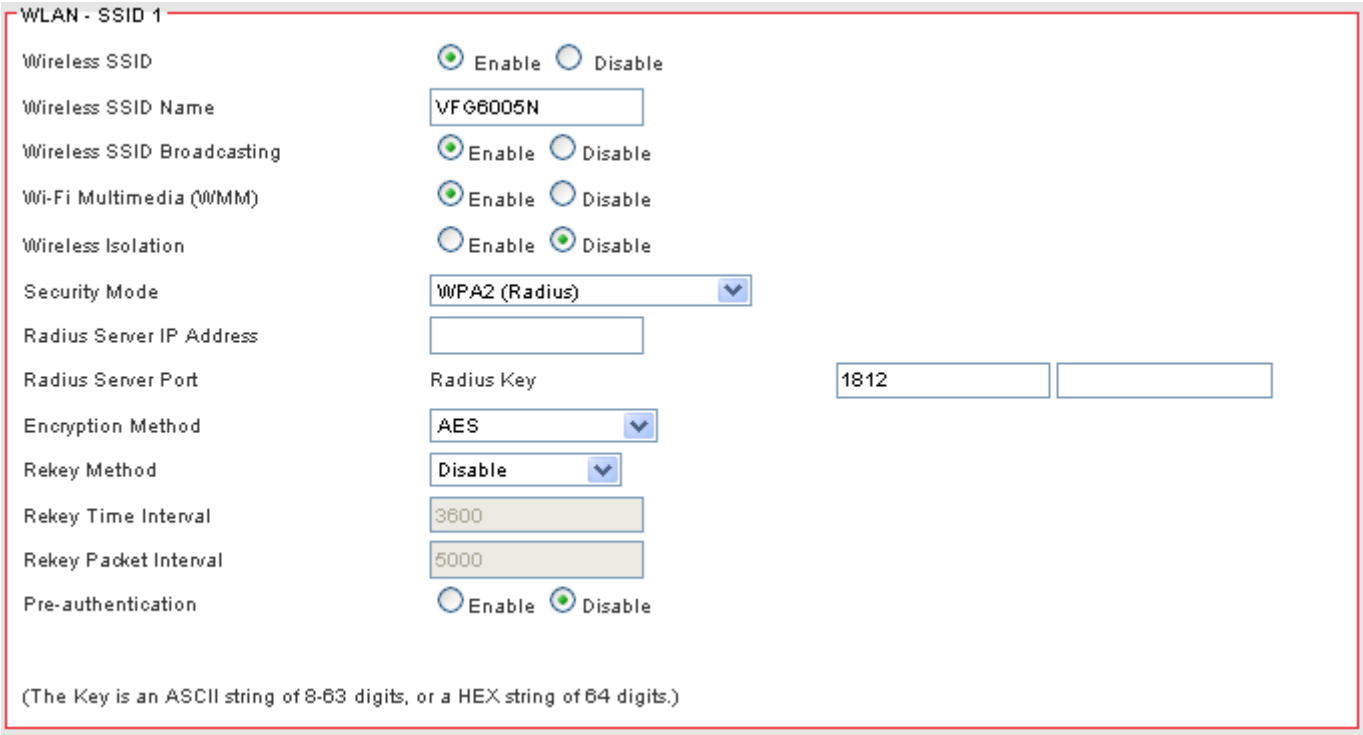
6.1.4 WPA Pre-shared Key / WPA2 Pre-shared Key



If WPA Pre-shared Key or WPA2 Pre-shared Key is selected, a Pre-shared Key is supposed to be set.

Key	Enter the Pre-Shared Key here. This key will be required for wireless users to connect to the SSID.
Encryption Method	Select TKIP, AES or Mixed (TKIP+AES). (AES recommended)

6.1.5 WPA / WPA2



If WPA or WPA2 is selected, the radius server information should be set accordingly.

Radius Server IP Address	Enter the RADIUS server's IP address.
Radius Server Port	Enter the RADIUS server's port number. The default port is 1812.
Radius Key	Enter the RADIUS server's IP Address.
Encryption Method	Select TKIP, AES or Mixed (TKIP+AES). (AES recommended)
Rekey Method	Select Disable/Time/Packet Number. Rekey by Time/Packet Number will require the user to re-authenticate with the RADIUS server after X Time/Packet Number, may increase overhead.
Rekey Time Interval	Enter Rekey Time Interval.
Rekey Packet Interval	Enter Rekey Packet Number.
Pre-Authentication	Select Enable/Disable for Pre-authentication. If enabled, this allows a wireless user to pre-authenticate with the AP before switching from another AP for quicker roaming.

6.2 ADVANCED SETUP

3. Click on [Wireless] – [Advanced] tab. You will see the following screen.

Wireless - Advanced

WLAN

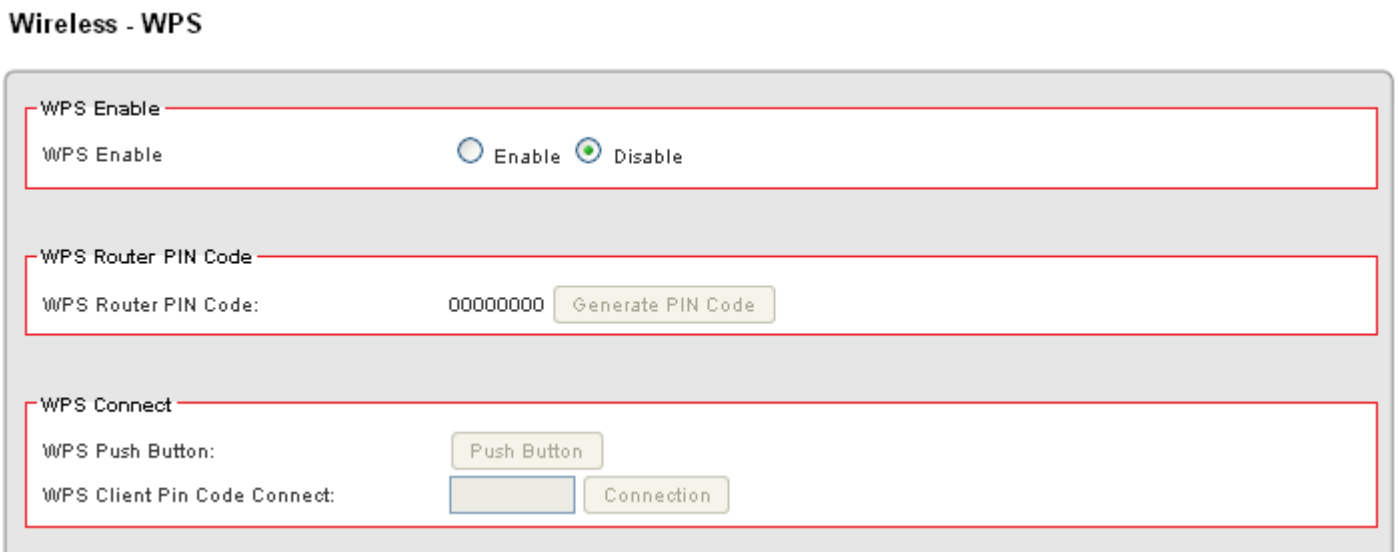
Fragmentation	2346	Bytes (256 ~ 2346)
RTS	2347	Seconds (1 ~ 2347)
DTim	1	(1 ~ 255)
Beacon Interval	100	Milliseconds (20 ~ 1024)
Header Preamble	Long	
TxMode	None	
MPDU	4	Microseconds
MSDU Aggregate	○ Enable	◉ Disable
Tx Burst	◉ Enable	○ Disable
Packet Aggregate	○ Enable	◉ Disable
HT Control Field	○ Enable	◉ Disable
Reverse Direction Grant	○ Enable	◉ Disable
Link Adapt	○ Enable	◉ Disable
Short Guard Interval(GI)	◉ Enable	○ Disable
Operation Mode	Mixed Mode	
HT Band Width	20/40	MHz
Block Ack Setup Automatically	◉ Enable	○ Disable
Block Ack Window Size	64	x16 Bits (1 ~ 64)
Reject Block Ack	○ Enable	◉ Disable
MCS	Auto	

4. Configure wireless advanced settings following the instructions below.

Fragmentation	Enter the fragmentation bytes. The default value is 2346 bytes.
RTS	Enter the RTS seconds. The default value is 2347 seconds.
DTim	Enter the DTim seconds. The default value is 1.
Beacon Interval	Enter the interval to send a beacon. The default value is 100 milliseconds.
Header Preamble	Select Long or Short header preamble.
TxMode	Select different transmission mode.
MPDU	MPDU data length. The transmission rate is increase when you choose a larger number, but usually the max value will be 4 in the wireless card
MSDU Aggregate	A kind of packet aggregation method, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
Tx Burst	Some 802.11g wireless card can supported this mode, and the transmission rate can be increased when enable this function.
Packet Aggregate	An aggregation method like A-MSDU, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
HT Control Field	Select Enable/Disable. It is useful when you need to debug the wireless network
Reverse Direction Grant	Select Enable/Disable. The response time can be shorter when enable this function.
Link Adapt	Select Enable/Disable. The function is use to dynamically change the modulation and encode mechanism between wireless devices.
Short Guard Interval (SGI)	Select Enable/Disable. Short GI can improve some transmission rate, but with less immunity when interference exist.
Operation Mode	Select Mixed mode or Greenfield. You may choose Greenfield mode to increase the transmission rate when you using 802.11n wireless network only.
HT Band Width	Using HT20MHz or HT20/40MHz
Block Ack Setup Automatically	Select Enable/Disable. If your Wifi Card supported Block Ack mechanism, it can improve the data transmission efficiency when enable this function.
Block Ack Window Size	Specify a Block Ack window size
Reject Block Ack	Select Enable to reject the request of BA from other Wireless device
MCS	Select transmission (connection) speed.

6.3 WPS – WIFI PROTECTED SETUP

1. Click on [Wireless] – [WPS] tab. You will see the following screen.



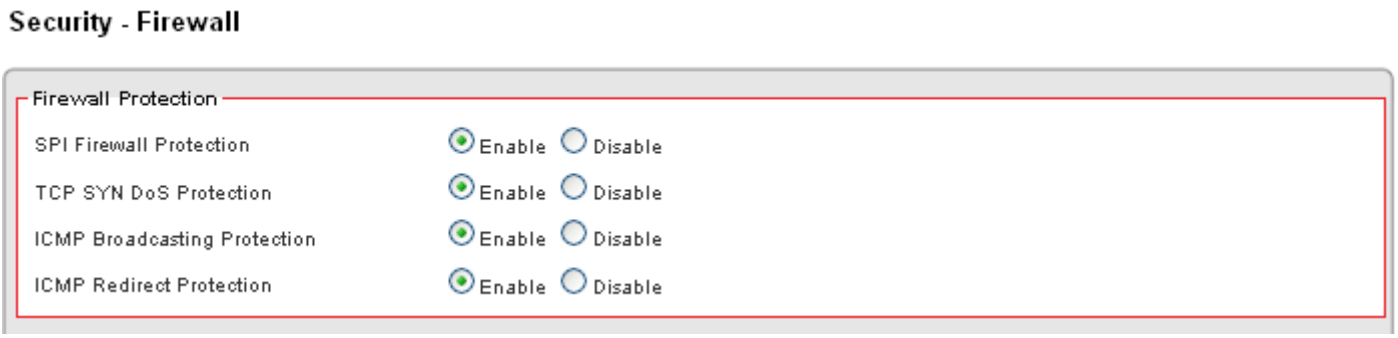
WPS Enable	Select Enable or Disable to activate or deactivate WPS.
WPS Router PIN Code	Click “Generate PIN Code” to automatically generate a random WPS PIN code.
WPS Push Button	Click this button to start the WPS process.
WPS Client PIN Code Connect	Use this to manually connect a client that has generated a PIN code.

To connect a computer using WPS, click **Push Button**. Then you will have two minutes to go to your computer, select the wireless network and connect. If your computer asks for a WPS PIN Code, that can be generated by clicking the **Generate PIN Code** button. If you are connecting to a device that has a WPS button, first click the WPS **Push Button** and then press the WPS button on that device within 2 minutes. This will connect the two devices together.

CHAPTER7 SECURITY SETTINGS

7.1 FIREWALL SETUP

1. Click on [Security] – [Firewall] tab. You will see the following screen.



2. Configure Security Settings following the instructions below.

SPI Firewall Protection	Select Enable to enable SPI Firewall Protection. Select Disable to disable SPI Firewall Protection.
TCP SYN DoS Protection	Check to enable TCP SYN DoS Protection. Uncheck to disable TCP SYN DoS Protection. TCP SYN DoS attack sends a flood of TCP/SYN packets. Each of these packets are like a connection request, causing the server to consume computing resources (e.g. memory, CPU) to reply and to continuously wait for the incoming packets. Without TCP SYN Dos Protection, the resources in the server will be easily consumed completely. This will then consequently result in the dysfunction of the server. The ZyXEL VFG6005 Series VPN Firewall Gateway is able to detect TCP SYN DoS attacks and limits the resource consumption by lowering the incoming request rate by fast recycling the resource. Therefore, the ZyXEL VFG6005 Series VPN Firewall Gateway is still able to serve normal traffic while it is under such an attack.
ICMP Broadcasting Protection	Check to enable ICMP Broadcasting Protection. Uncheck to disable ICMP Broadcasting Protection. ICMP broadcasting attack is a type of DoS attacks. A flood of ICMP broadcasting packets is generated and sent to a server (like the ZyXEL VFG6005 Series VPN

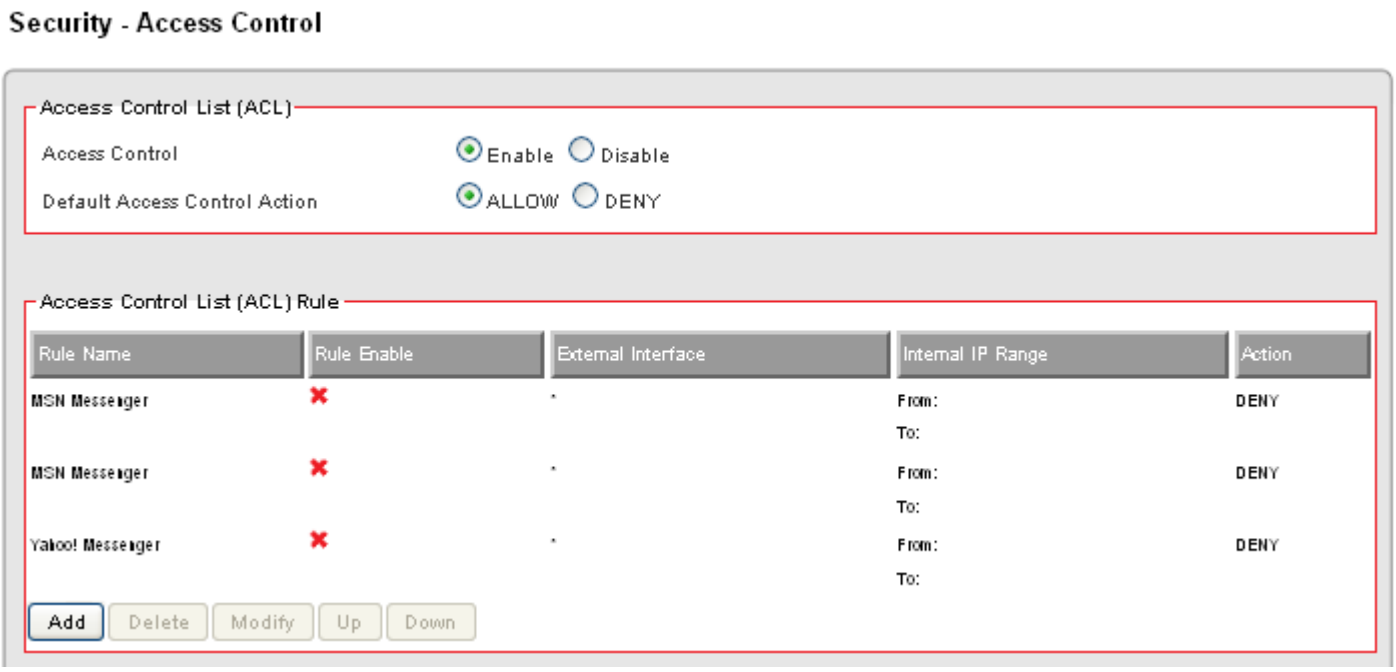
	Firewall Gateway). Consequently, this server will suffer from a huge amount of interruptions and consumption of computing resources. The ZyXEL VFG6005 Series VPN Firewall Gateway is able to stop responding to ICMP broadcasting echo packets in order to avoid a potential ICMP broadcasting DoS attack.
ICMP Redirect Protection	Check to enable ICMP Redirect Protection. Uncheck to disable ICMP Redirect Protection. An ICMP redirect message is a way to change the existing routing path. Generally, ICMP redirect packets should not be sent, and so when there is the occurrence that ICMP redirect packets are sent, it is important to note that it is very likely to be used as a means for a network attack.

7.2 ACCESS CONTROL LIST (ACL) SETUP

7.2.1 ACL Settings

1. Click on [Security] – [Access Control] tab. You will see the following screen.

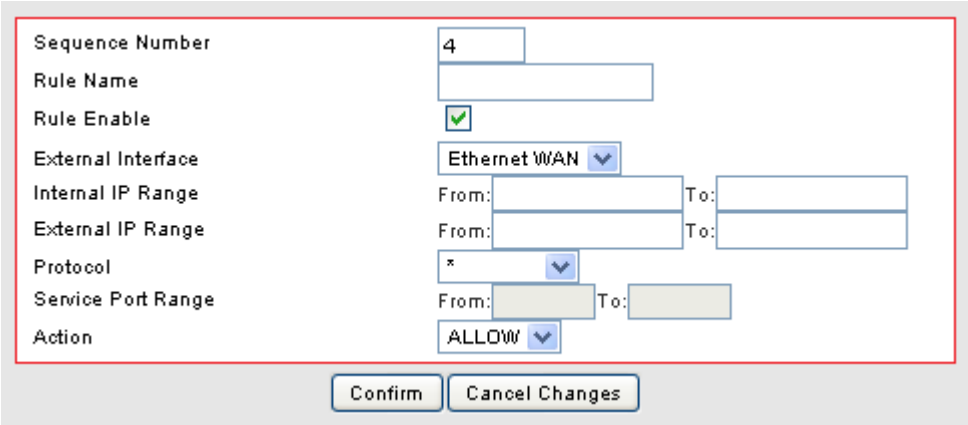
Please do not change the parameters unless you wish to customize it by yourself.



2. Configure Access Control List (ACL) Settings following the instructions below.

ACL	Select Enable to enable ACL. Select Disable to disable ACL.
Default ACL Action	Check Enable to enable a specific MAC Filter rule. Uncheck Enable to disable a specific MAC Filter rule. Type the MAC address to permit a device to access to the network. * Enabling MAC filtering blocks all MAC addresses which are not listed in the MAC Filter Rule. Be aware that adding the MAC address of your managing computer is required in order to access to the ZyXEL VFG6005 Series VPN Firewall Gateway.

3. Click on [Add] tab. You will see the following screen.



4. Configure [Add Access Control List (ACL)] Settings following the instructions below

Sequence Number	This defines the sequence of the ACL rules. If a packet fits the conditions set by the ACL rules, the packet will then be sorted according to the first ACL rule from the top of the list.
Rule Name	Name of the ACL rule.
Rule Enable	Enable/Disable this ACL rule
External Interface	Please select which External Interface (WAN1 or WAN2) you want a packet to go through, IF the packet fits the condition of this ACL rule.
Internal IP Range	Set up the internal IP range for this ACL rule.
External IP Range	Set up the external IP range for this ACL rule.
Protocol	Set up the protocol (TCP or UDP) for the ACL to be enabled.
Service Port Range	Set up the Service Port Range (e.g., HTTP is TCP/80) for the ACL to be enabled.
Action	Select ALLOW / DENY。

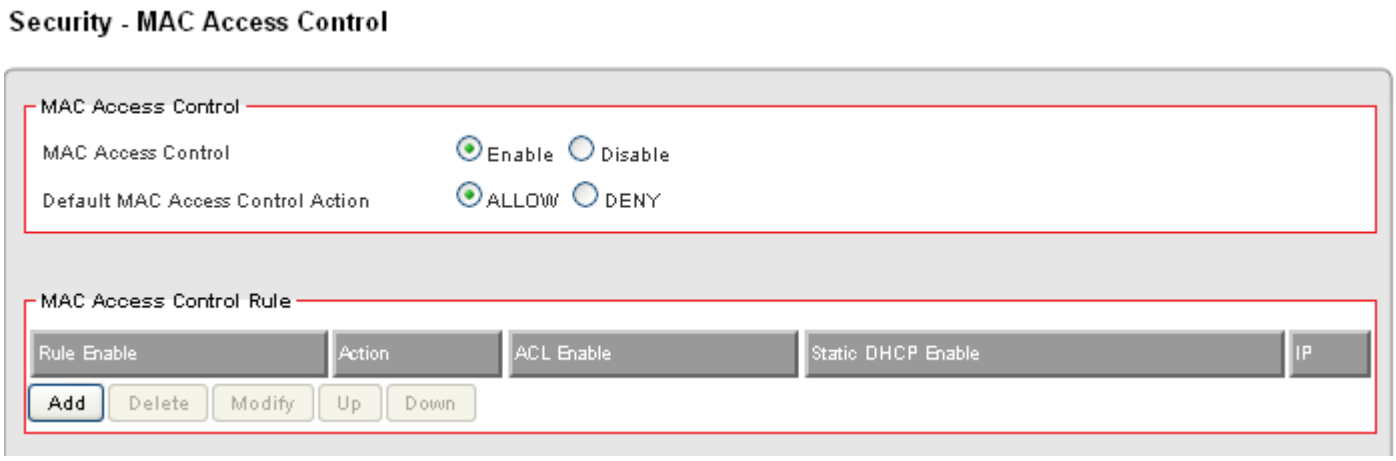
5. Example: Filter and block MSN usage.

For example, a company does not wish to allow employees to use MSN. The system administrator can set up an ACL action: rejecting the traffic going out to External IP Range at 207.46.110.*/24.

Rule Name	MSN Blocking
Rule Enable	Enable
External Interface	* (All complies)
Internal IP Range	Keep it blank (All complies)
External IP Range	207.46.110.1:207.46.110.1.254 (IP address range for MSN server)
Protocol	TCP
Service Port Range	Keep it blank (All complies)
Action	DENY

7.3 MAC ACCESS CONTROL SETUP

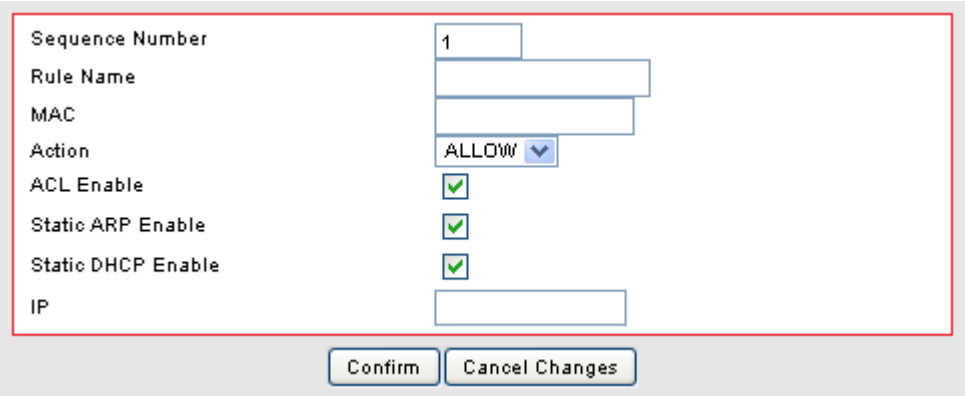
1. Click on [Security] – [MAC Access Control] tab. You will see the following screen.



2. Configure ACL Settings following the instructions below.

MAC Access Control	Choose Enable/Disable to enable/disable MAC access Control
Default MAC Access Control Action	The default ACL action of the ACL rules. When you add the individual rules, it can be viewed as exceptions and take effects relating to the default action. If the action of the adding rule is the same as the default action, then this rule will not work.

3. Click on [Add] tab. You will see the following screen.



4. Example: Bind IP to a MAC

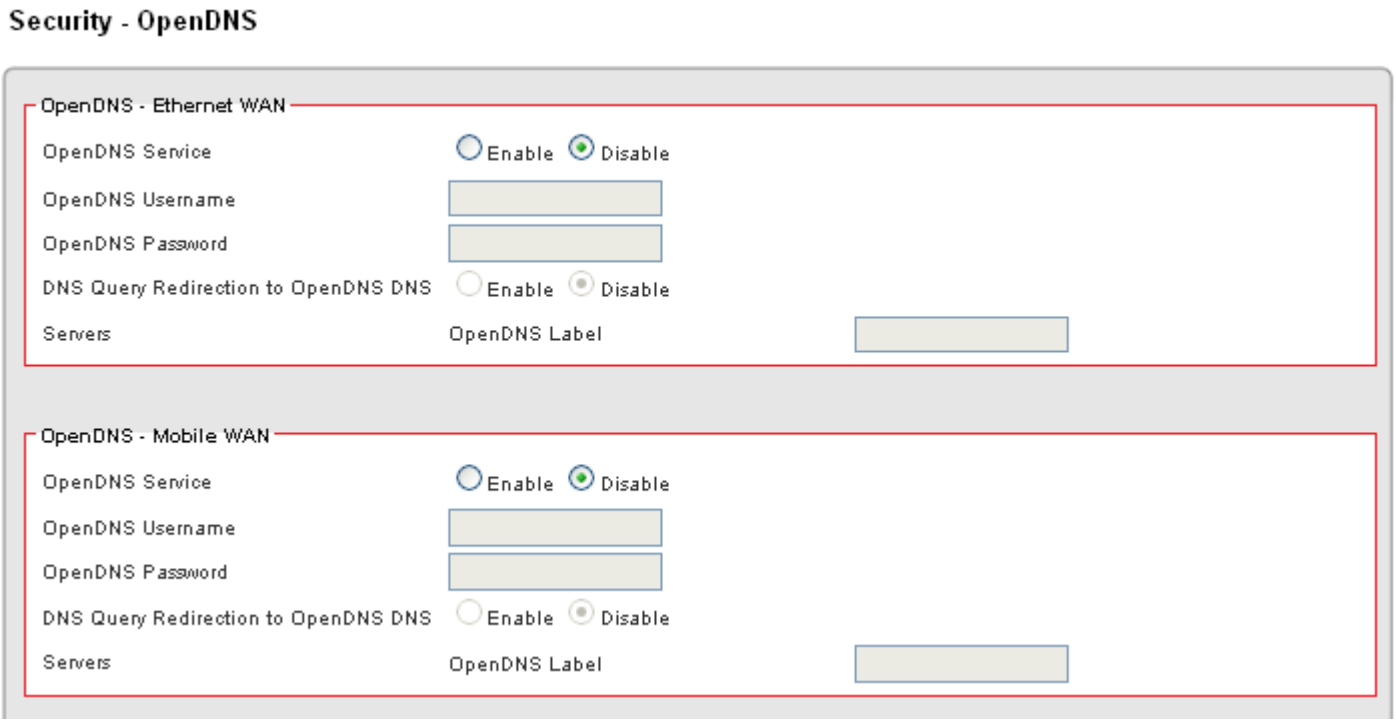
If users need to bind an IP to a specified MAC (network device), one can follow the settings as below.

Sequence Number	User1
Rule Name	Enable
MAC	00:33:44:55:66:77
Action	Allow Access
ACL Enable	Enable
Static ARP Enable	Enable
Static DHCP Enable	Enable
IP	192.168.10.100

7.4 OpenDNS SETUP

7.4.1 OpenDNS Settings

1. Click on [Security] – [OpenDNS] tab. You will see the following screen.

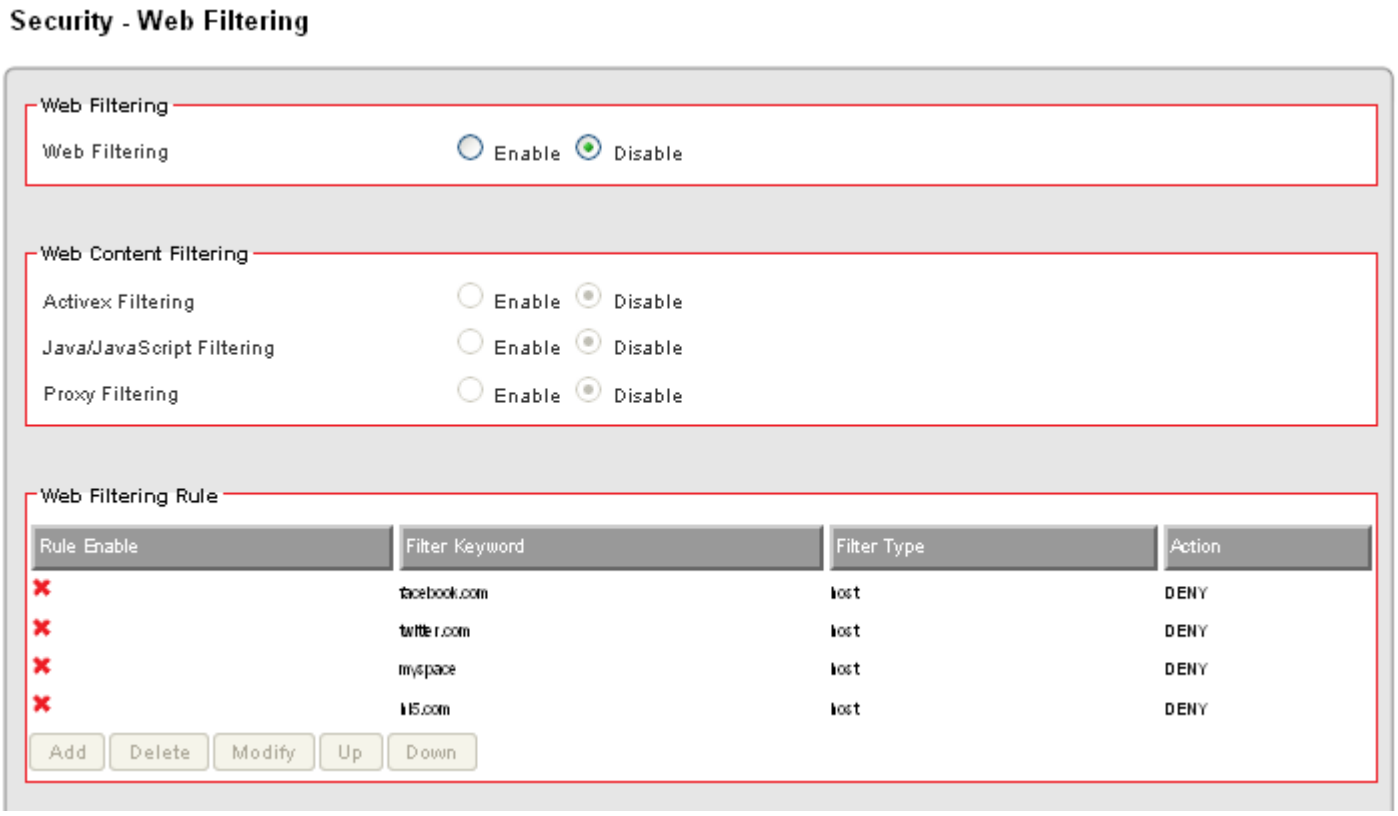


2. Configure OpenDNS Settings following the instructions below.

OpenDNS Service	Choose Enable/Disable to enable/disable OpenDNS
OpenDNS Username	Enter OpenDNS user name.
OpenDNS Password	Enter OpenDNS password.
DNS Query Redirection to OpenDNS DNS Servers	Choose Enable/Disable to enable/disable the data flow redirect to the OpenDNS Server. Users can get advanced content filtering function through the setting
OpenDNS Label	Enter the OpenDNS Label

7.5 WEB FILTERING SETUP

1. Click on [Security] – [Web Filtering] tab. You will see the following screen.

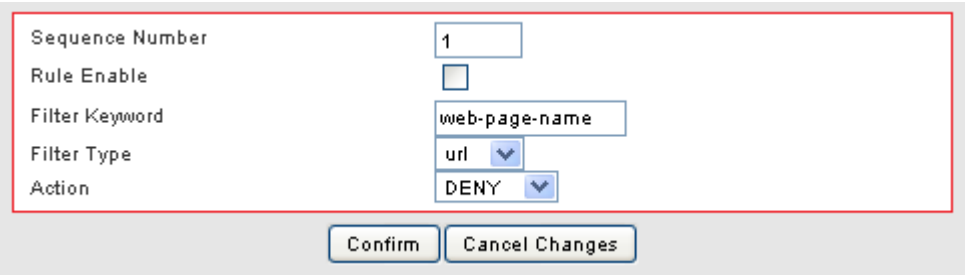


2. Configure Web Filtering Settings following the instructions below.

Web Filtering	Choose Enable/Disable to enable/disable Web Filtering
Activex Filtering	Choose Enable/Disable to enable/disable Activex Filtering
Java/JavaScript Filtering	Choose Enable/Disable to enable/disable Java/JavaScript Filtering
Proxy Filtering	Choose Enable/Disable to enable/disable Proxy Filtering

7.5.1 Added Web Filtering Rules

1. Click on [Add] tab. You will see the following screen.



2. Configure Web Filtering Settings following the instructions below

Sequence Number	This defines the sequence (priority) of all the Web Filtering rules.
Rule Enable	Choose Enable/Disable to enable/disable Web Filtering rule
Filter Keyword	Enter the Keyword
Filter Type	Choose URL or Sever
Action	Select ALLOW / DENY。

3. Example: Block a URL with Keyword

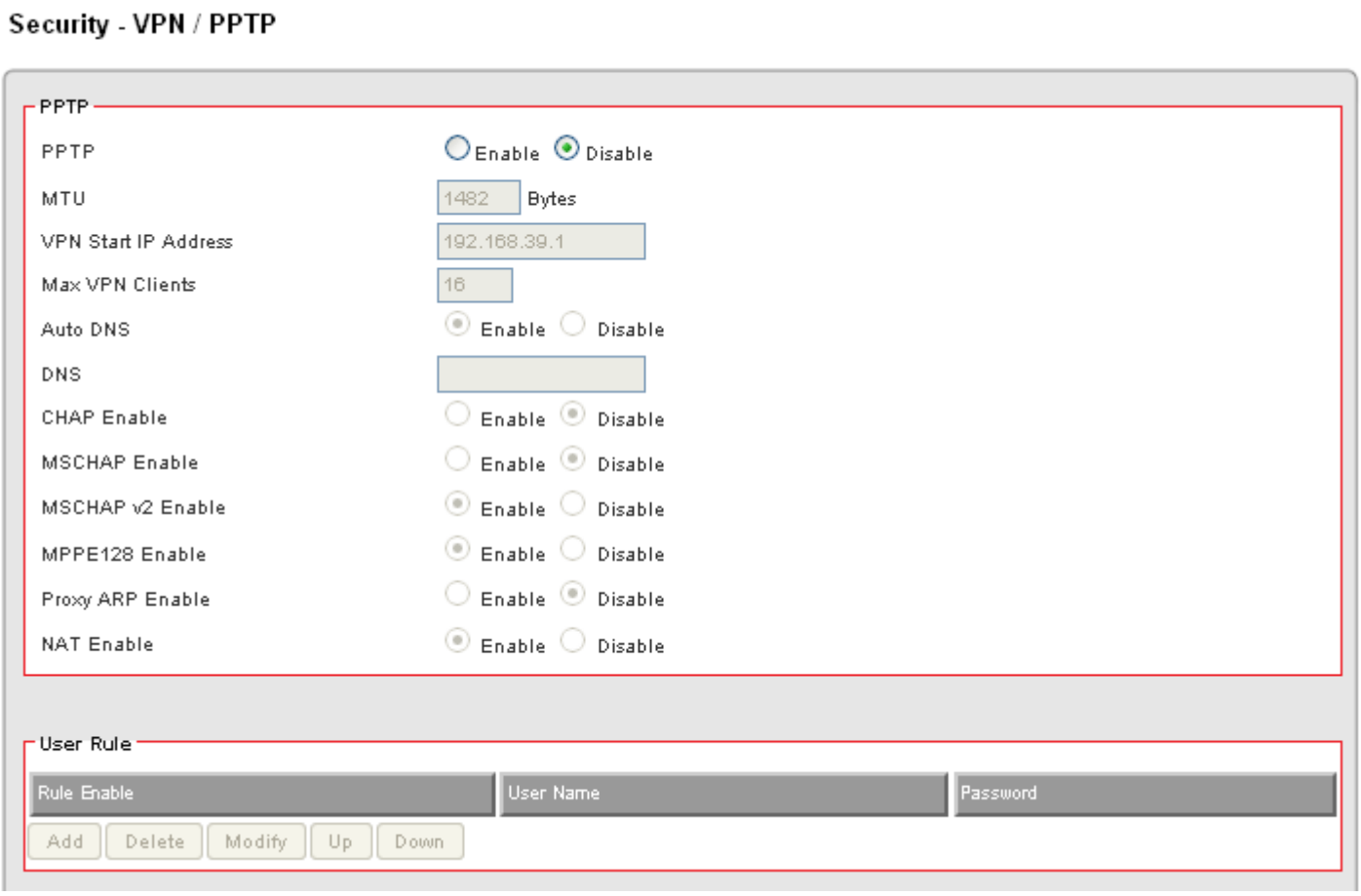
If one need to block Facebook related web page, can follow the settings as below

7.6 VPN / PPTP SETUP

7.6.1 VPN / PPTP Settings

PPTP VPN allows you to create a secure VPN connection remotely to your LAN. PPTP can allow you to connect using built in software clients such as Windows VPN client or smart devices such as Android phones/tablets, iPhones or iPads.

1. Click on [Security] – [VPN / PPTP] tab. You will see the following screen.

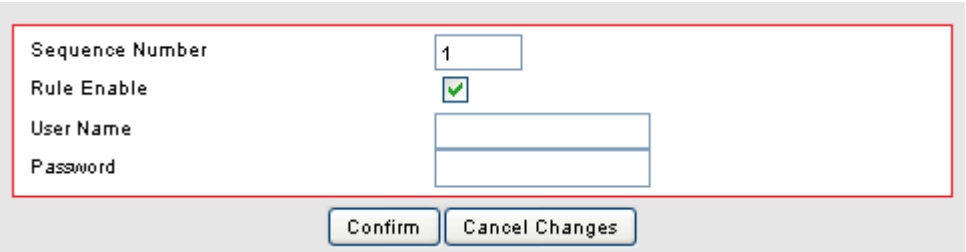


2. Configure PPTP Settings following the instructions below.

PPTP	Choose Enable/Disable to enable/disable L2TP.
MTU	Enter MTU value. The default value is 1482 bytes.
VPN Start IP Address	Enter the VPN start IP address. The default value is 192.168.39.1.
Max VPN Clients	Enter the max VPN clients.
Auto DNS	Choose Enable/Disable to enable/disable Auto DNS.
DNS	Enter DNS server if you choose Disable for Auto DNS.
CHAP Enable	Choose Enable/Disable to enable/disable CHAP for VPN authentication.
MSCHAP Enable	Choose Enable/Disable to enable/disable MSCHAP for VPN authentication.
MSCHAP2 Enable	Choose Enable/Disable to enable/disable MSCHAP2 for VPN authentication.
MPP128 Enable	Choose Enable/Disable to enable/disable MPP128 encryption.
Proxy ARP Enable	Choose Enable/Disable to enable/disable Proxy ARP.
NAT Enable	Choose Enable/Disable to enable/disable NAT.

7.6.2 Add VPN / PPTP Rule

1. Click on [Add] tab. You will see the following screen.



2. Configure [Add PPTP] Settings following the instructions below.

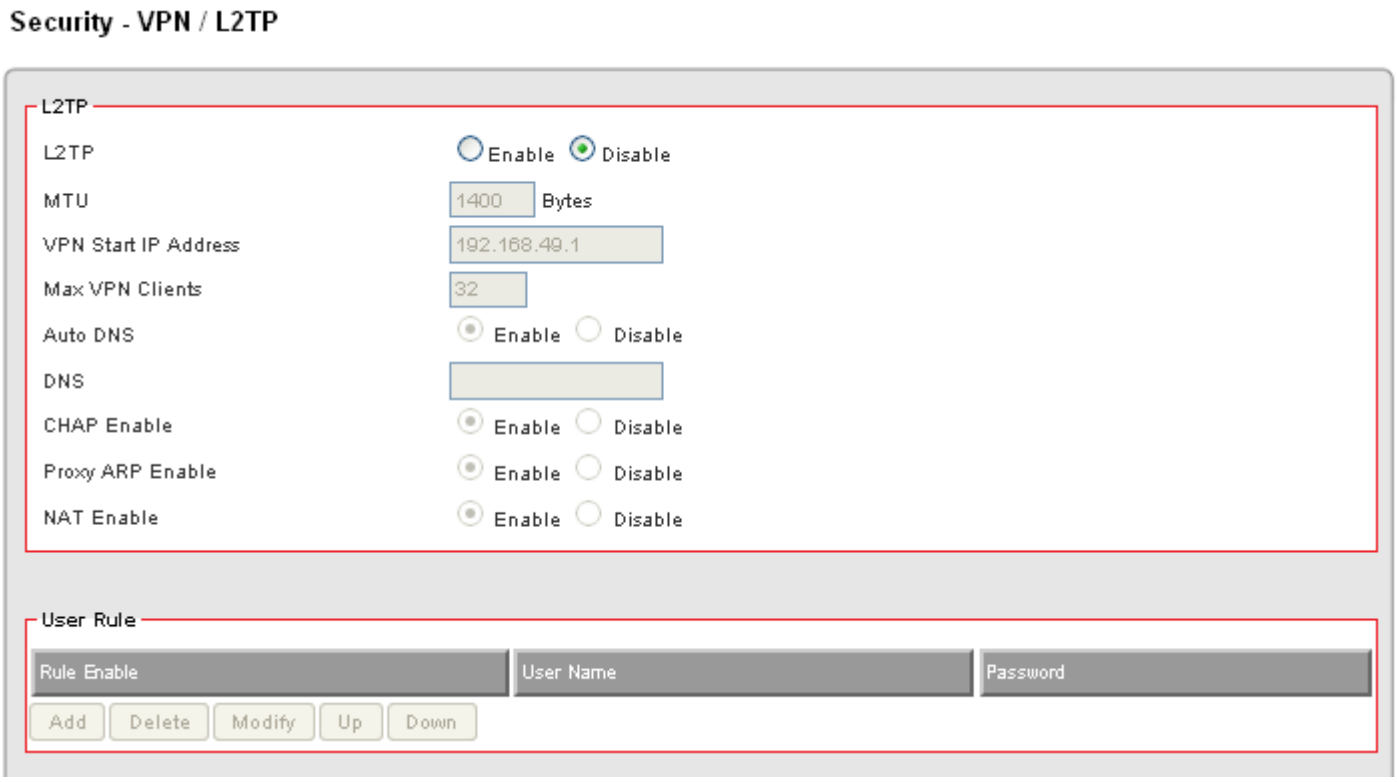
Sequence Number	This defines the sequence of the PPTP rules.
Rule Enable	Enable/Disable this PPTP rule
User Name	Enter PPTP user name.
Password	Enter PPTP password.

7.7 VPN / L2TP SETUP

7.7.1 VPN / L2TP Settings

L2TP allows you to create an insecure VPN connection to your LAN. Because L2TP is insecure, we suggest that you use PPTP or L2TP over IPSec. Also both L2TP and L2TP over IPSec have the restriction that the VPN client cannot be behind a NAT router and must have a routable public IP address.

1. Click on [Security] – [VPN / L2TP] tab. You will see the following screen.

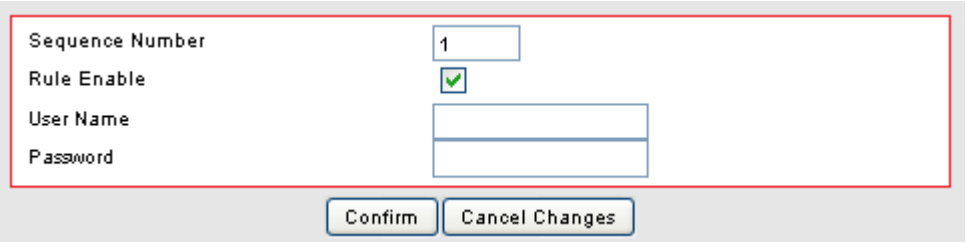


2. Configure PPTP Settings following the instructions below.

L2TP	Choose Enable/Disable to enable/disable L2TP.
MTU	Enter MTU value. The default value is 1482 bytes.
VPN Start IP Address	Enter the VPN start IP address. The default value is 192.168.39.1.
Max VPN Clients	Enter the max VPN clients.
Auto DNS	Choose Enable/Disable to enable/disable Auto DNS.
DNS	Enter DNS server if you choose Disable for Auto DNS.
CHAP Enable	Choose Enable/Disable to enable/disable CHAP for VPN authentication.
Proxy ARP Enable	Choose Enable/Disable to enable/disable Proxy ARP.
NAT Enable	Choose Enable/Disable to enable/disable NAT.

7.7.2 Add VPN / L2TP Rule

3. Click on [Add] tab. You will see the following screen.



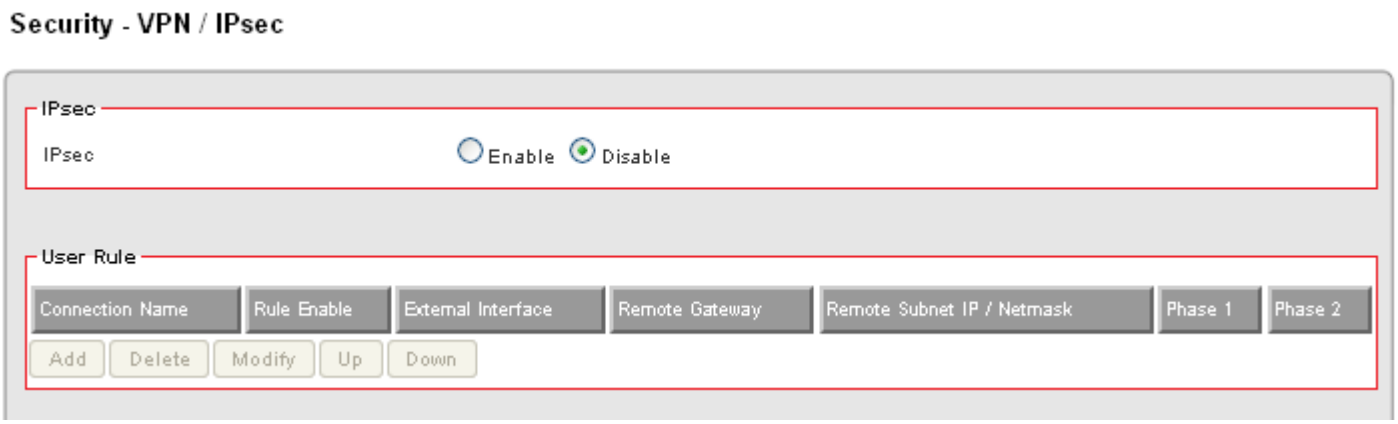
4. Configure [Add PPTP] Settings following the instructions below.

Sequence Number	This defines the sequence of the PPTP rules.
Rule Enable	Enable/Disable this PPTP rule
User Name	Enter PPTP user name.
Password	Enter PPTP password.

7.8 VPN / IPsec SETUP

7.8.1 VPN / IPsec Settings

1. Click on [Security] – [VPN / IPsec] tab. You will see the following screen.

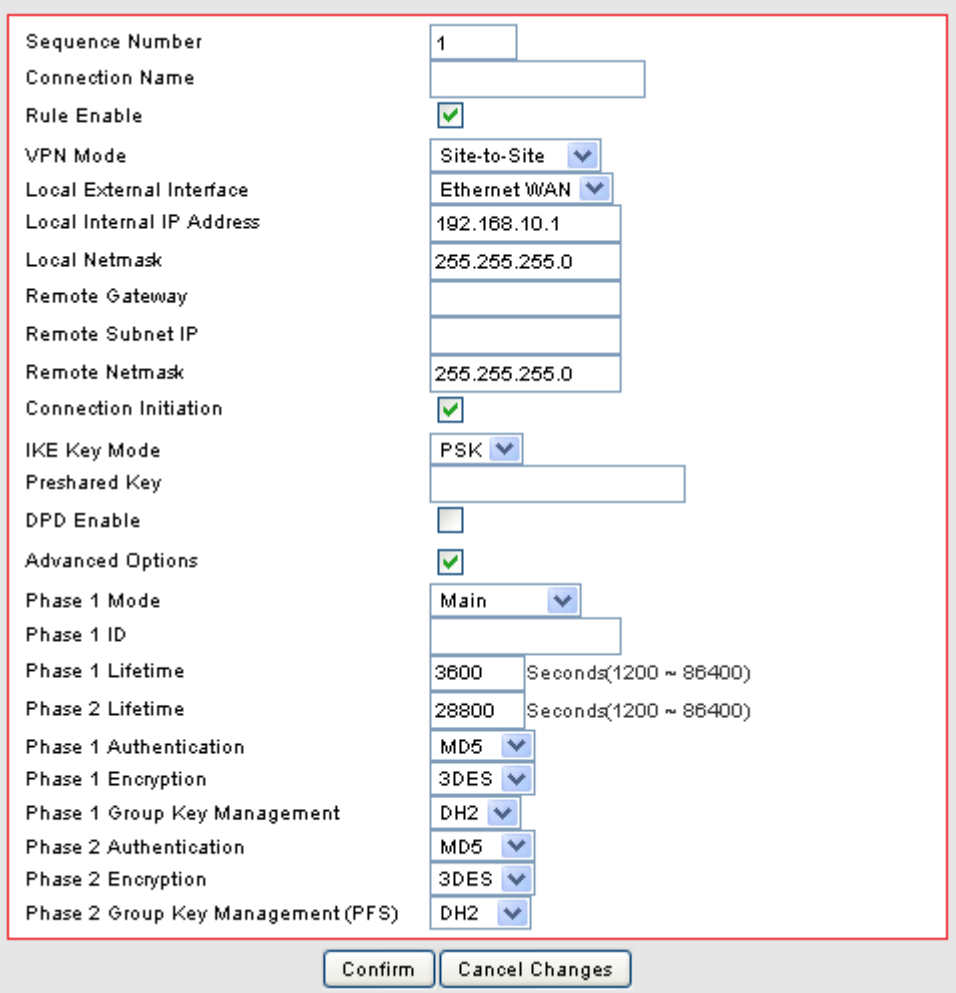


2. Configure IPsec Settings following the instructions below.

IPsec	Select Enable/Disable to enable/disable IPsec.

7.8.2 Add VPN / IPsec Rule

1. Click on [Add] tab. You will see the following screen.



2. Configure [Add - IPsec] Settings following the instructions below.

Sequence Number	This defines the sequence of the IPsec rules.
Connection Name	Name of the IPsec rule.
Rule Enable	Enable/Disable this IPsec rule
VPN Mode	Net-to-Net or Road Warrior
Local External Interface	Select the external WAN for the local VPN gateway.
Local Internal IP Address	Select the subnet IP address for the VPN gateway.
Local Netmask	Select the netmask for the local VPN gateway.
Remote Gateway	Enter the IP address or domain name of the remote VPN gateway. This option is needed in Net-to-Net mode.
Remote Subnet IP	Enter the subnet IP address of the remote VPN gateway. This option is needed in Net-to-Net mode.
Remote Netmask	Enter the subnet netmask of the remote VPN gateway. This option is needed in Net-to-Net mode.
Connection Initiation	Check the local VPN gateway to initiate the connection. This option is needed in Net-to-Net mode.
IKE Key Mode	PSK.
Preshared Key	Enter the preshared key. The key should be at least 8-digit ASCII string.
L2TP Enable	Check the local VPN gateway to enable L2TP. This option is needed in Road Warrior mode.
Advanced Options	Check it if you need to configure the advanced options.
Phase 1 Mode	Main.
Phase 1 ID	Enter the phase 1 ID.
Phase 1 Lifetime	Enter the phase 1 lifetime. This value is between 3600 and 28800 seconds.
Phase 2 Lifetime	Enter the phase 2 lifetime. This value is between 3600 and 28800 seconds.
Phase 1 Authentication	Select the phase 1 authentication as MD5 or SHA1. (SHA1 recommended)
Phase I Encryption	Select the phase 1 encryption as DES, 3DES or AES. (AES recommended)
Phase 1 Group Key Management	Select the phase 1 group key management as DH1, DH2 or DH5.
Phase 2 Authentication	Select the phase 2 authentication as MD5 or SHA1. (SHA1 recommended)
Phase 2 Encryption	Select the phase 2 encryption as DES, 3DES or AES. (AES recommended)
Phase 2 Group Key Management	Select the phase 2 group key management as DH1, DH2 or DH5.

CHAPTER8 APPLICATIONS SETTINGS

8.1 PORT RANGE FORWARD SETUP

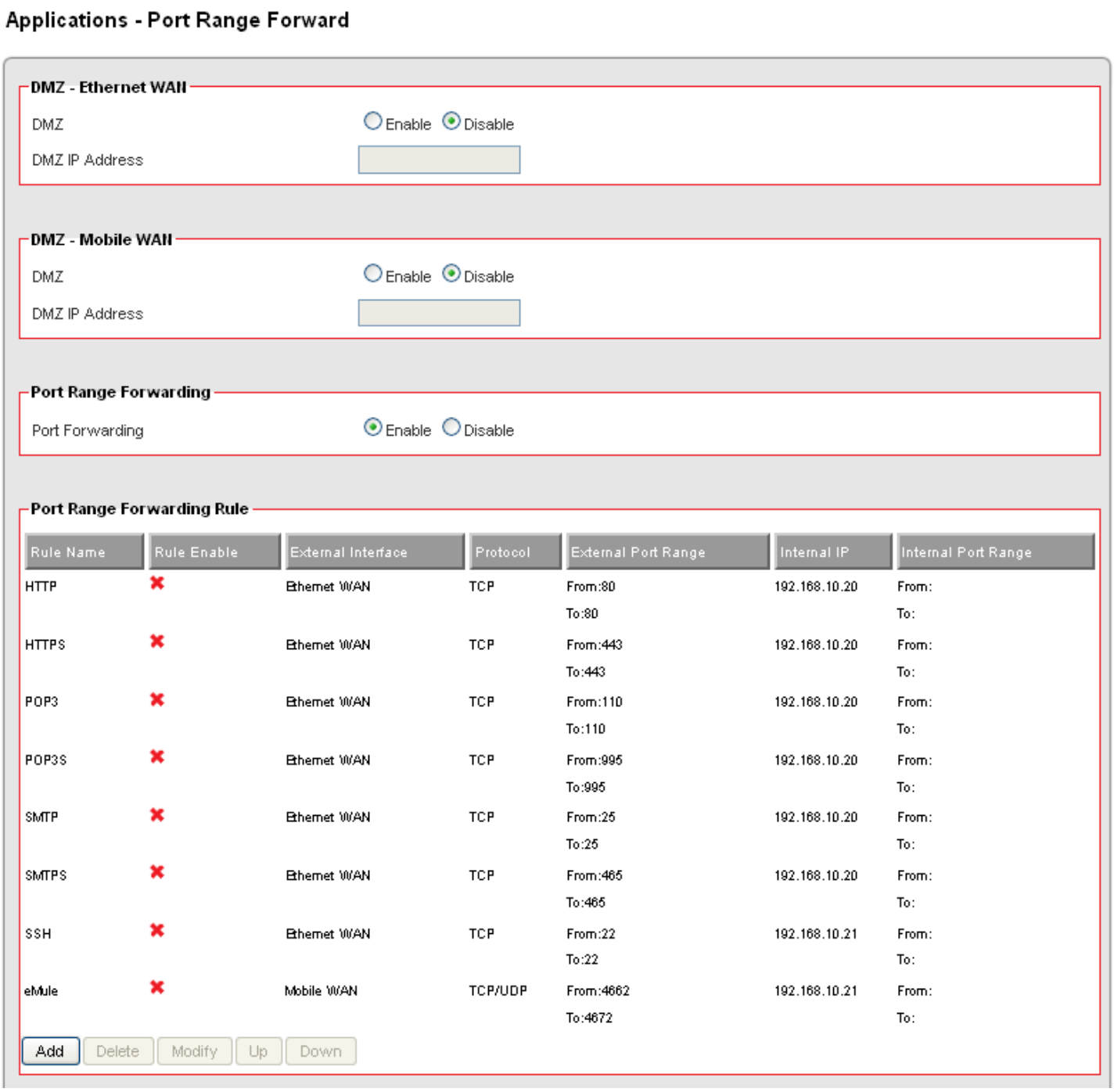
By activating the port range forwarding function, remote users can access the local network via the public IP address. Users can assign a specific external port range to a local server. Furthermore, users can specify an internal port range associated in a port range forwarding rule. When the ZyXEL VFG6005 Series VPN Firewall Gateway receives an external request to access any one of the configured external ports, it will redirect the request to the corresponding internal server and change its destination port to one of the internal ports specified. Therefore, if users do not wish for destination port to be changed for a request, the internal port range should be left empty.

Certain applications in a LAN are available only after activating the port range forwarding, including servers and online gaming. When an Internet request wants to access a port, the ZyXEL VFG6005 Series VPN Firewall Gateway will dispatch it to the IP specified. Due to security reasons, users are suggested to limit the use of port range forwarding, and cancel it when the application is not used.

By enabling DMZ Host Function, you can set up a DMZ host at a particular computer exposed to the Internet. In this way, some applications, especially online games (if the traffic port numbers of the applications are always changing), can be easily accessed.

8.1.1 Port Range Forward Settings

1. Click on [Applications] – [Port Range Forward] tab. You will see the following screen.



2. Configure [DMZ] Settings following the instructions below

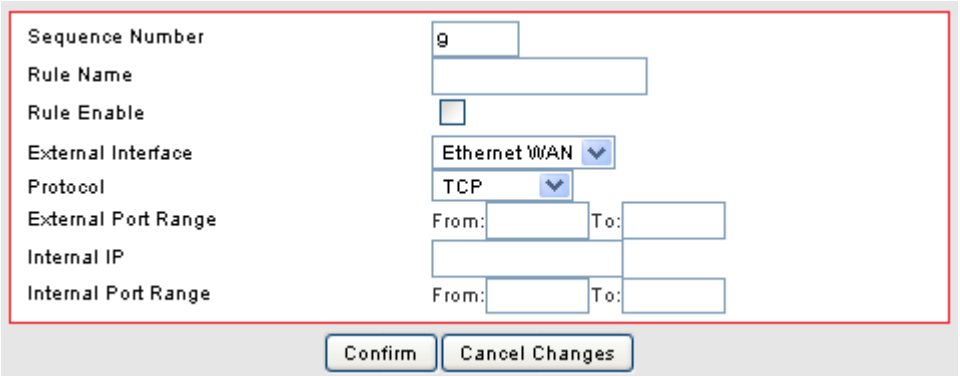
DMZ	Select Enable to enable DMZ function. Select Disable to disable DMZ function.
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port / Public IP address above.

3. Configure [Port Range Forwarding] Settings following the instructions below

Port Forwarding	Select Enable / Disable to enable/disable Port Forwarding

8.1.2 Add Port Range Forwarding Rule

1. Click on [Add] tab. You will see the following screen.



2. Configure [Add Port Range Forwarding Rule] Settings following the instructions below

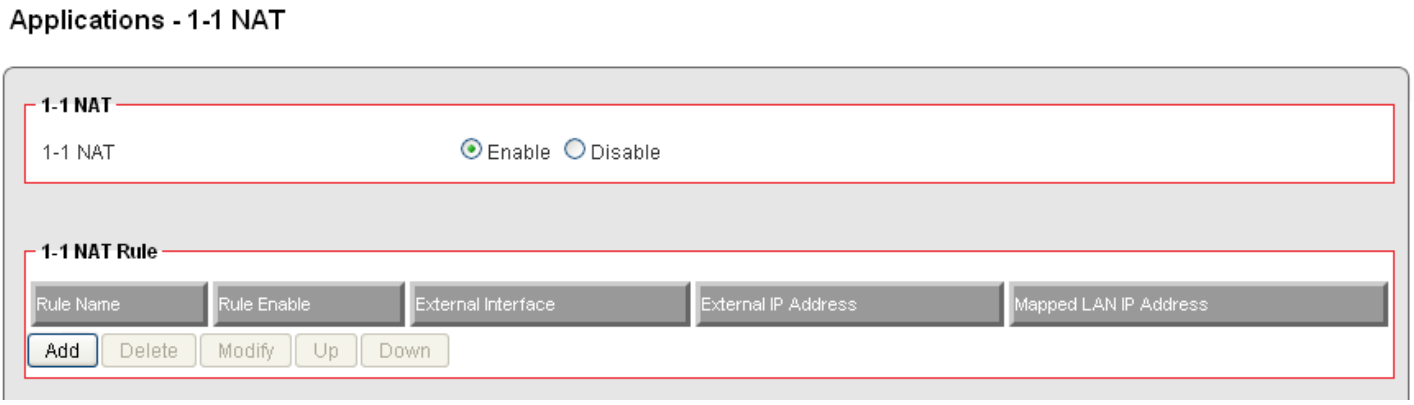
Sequence Number	This defines the sequences (priorities) of the port forwarding rules. If a packet fits the conditions setup by the port forwarding rules, the packet will then be forwarded according to the 1st rule from the top of the list.
Rule Name	Enter the name of the port forwarding rule.
Rule Enable	Check/Uncheck to enable/disable this port forwarding rule.
External Interface	Choose WAN1 or WAN2 as the External port forwarding interface.
Protocol	Choose TCP, UDP or TCP/UDP for the rule to be applied.
External Port Range	Set up the External Port Range for the rule to be applied.
Internal IP	Set up the Internal IP for the rule to be applied.
Internal Port Range	Set up the Internal Port Range for the rule to be applied.

8.2 1-1 NAT

1-1 NAT allows you to map an external Public IP address to an internal LAN IP address. If you have a range of Public IP addresses assigned by your ISP, you can use each of those IP addresses to assign to a specific LAN server. For example, you can assign a Public IP address to a Web Server or a Mail Server that needs to be accessed publicly through the Internet.

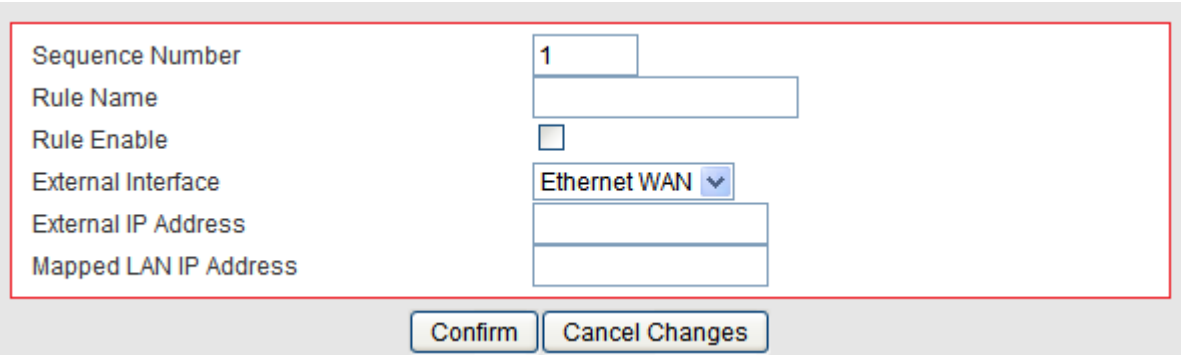
8.2.1 1-1 NAT Settings

1. Click on [Applications] – [Virtual Hosts] tab. You will see the following screen.



8.2.2 Add 1-1 NAT Rule

1. Click on [Add] tab. You will see the following screen.



2. Configure [Add Port Range Forwarding Rule] Settings following the instructions below

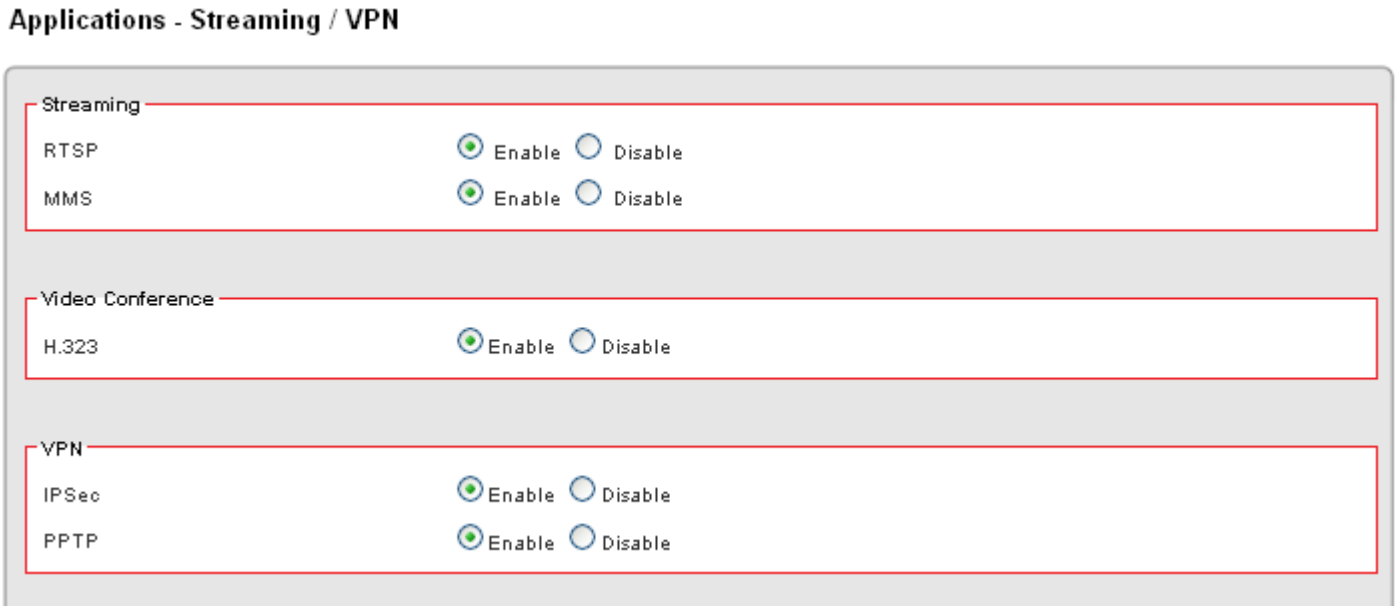
Sequence Number	This defines the sequences (priorities) of the port forwarding rules. If a packet fits the conditions setup by the port forwarding rules, the packet will then be forwarded according to the 1st rule from the top of the list.
Rule Name	Enter the name of the virtual hosts rule.
Rule Enable	Check/Uncheck to enable/disable this port forwarding rule.

External Interface	Choose Ethernet WAN or Mobile WAN as the External virtual host interface.
External IP Address	Enter the External IP Address.
Mapped LAN IP Address	Enter the Mapped LAN IP Address this External IP Address will be mapped to.

8.3 STREAMING/VPN PASS-THROUGH

You can enhance your media streaming quality by enabling RTSP, MSS, and H.323 protocols. Moreover, VPN Pass-through functionality can also be enabled.

1. Click on [Applications] – [Streaming / VPN] tab. You will see the following screen.



2. Configure [Streaming] Settings following the instructions below.

RTSP	Select Enable/Disable to enable/disable RTSP
MMS	Select Enable/Disable to enable/disable MMS

3. Configure [Video Conference] Settings following the instructions below

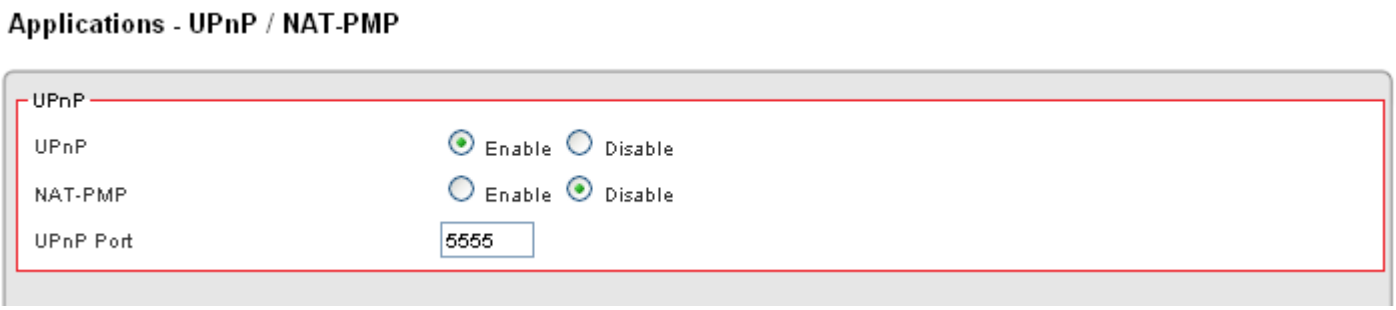
H.323	Select Enable/Disable to enable/disable H.323

4. Configure [VPN] Settings following the instructions below

IPSec Pass-through	Select Enable/Disable to enable/disable IPSec Pass-through
PPTP Pass-through	Select Enable/Disable to enable/disable PPTP Pass-through

8.4 UPnP/NAT-PMP SETUP

1. Click on [Applications] – [UPnP / NAT-PMP] tab. You will see the following screen.



2. Configure [UPnP] Settings following the instructions below

UPnP	Select Enable/Disable to enable/disable UPnP
NAT-PMP	Select Enable/Disable to enable/disable NAT-PMP
UPnP Port	Enter the number for UPnP port.

CHAPTER9 DYNAMIC BANDWIDTH MANAGEMENT

9.1 DBM SETUP

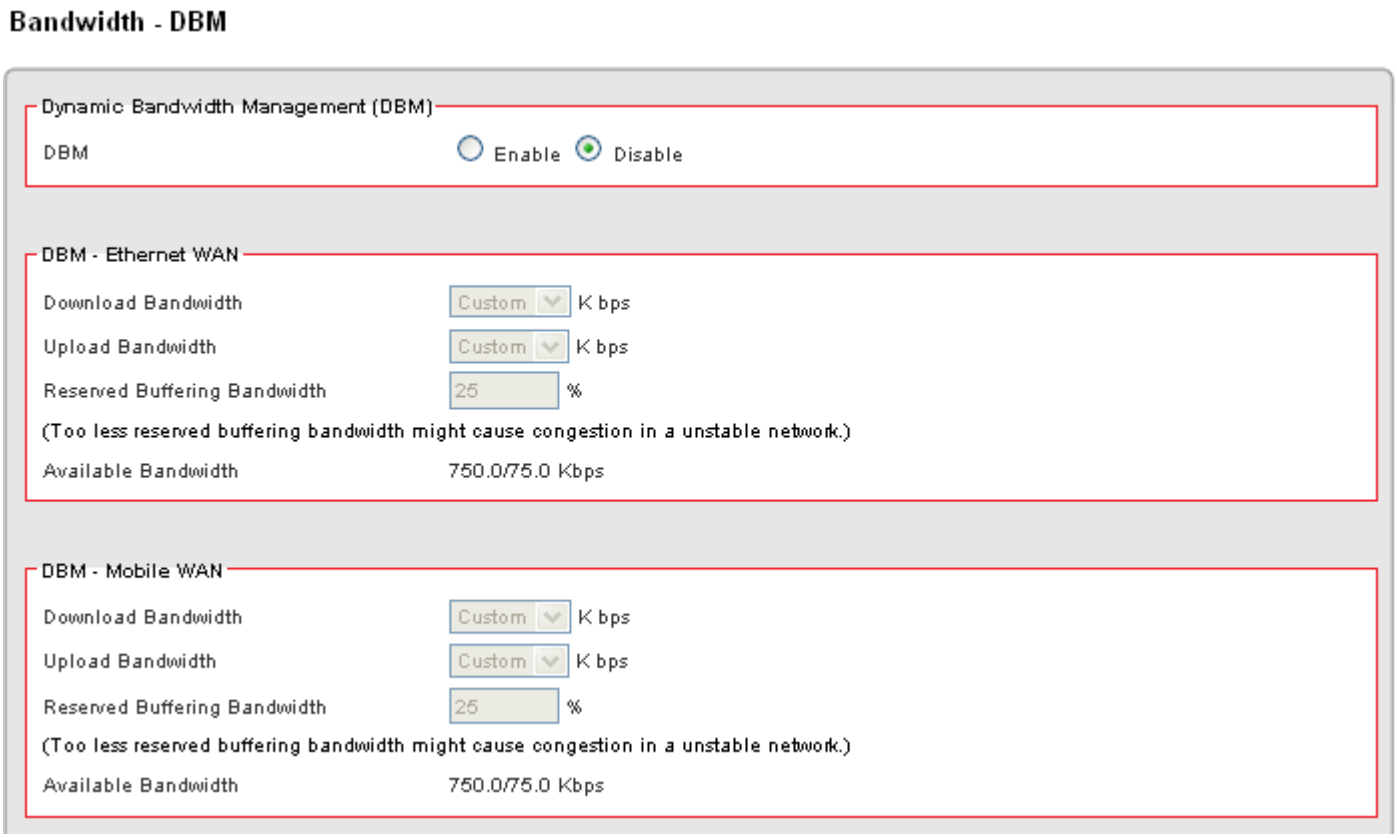
Bandwidth Management provides two powerful and unique mechanisms to manage bandwidth: Static Bandwidth Management (SBM) and Dynamic Bandwidth Management (DBM). SBM provides users with the option to allocate a fixed amount of bandwidth for a specific computer or a particular application, while DBM intellectually manages the rest of the bandwidth while all the time satisfying the complicated bandwidth requirements/settings of SBM.

DBM automatically and consistently monitors bandwidth usage, prioritizes traffic, and allocates bandwidth to all users and applications. Real-time applications such as **VoIP**, **online gaming**, and **video conferencing**, are granted a higher priority for bandwidth usage. On the other hand, applications such as **P2P** and **FTP** are given a lower priority. However, when P2P software is the only application running on the network, DBM is able to provide an efficient allocation and ensure that no bandwidth is wasted by being able to recognize that it is the only application running. Once real-time applications join the network, these applications will then immediately have a higher priority to use bandwidth than P2P software. Therefore, users can play online games, stream network videos, listen to network radio, chat with friends, send e-mails, and run P2P applications, all at the same time with no disturbances!

9.1.1 DBM Settings

The essential configuration needed by Bandwidth Management is to specify accurately the bandwidth you have. Bandwidth Management would then dispatch bandwidth according to this information. Please Note: Improper bandwidth assignment may cause Bandwidth Management to work ineffectively.

1. Click on [Bandwidth] – [Bandwidth Management] tab. You will see the following screen.



2. Bandwidth Settings:

Please adjust your bandwidth type according to your bandwidth (download/upload) subscribed from your ISP. Due to the unstable nature of network bandwidth supported by ISP, users are recommended to reserve a portion of bandwidth for buffering usage, and Bandwidth Management would then arrange the reserved bandwidth under heavy traffic.

Bandwidth Type (Download/Upload)	Select the correct bandwidth type according to your Internet service subscription. If the bandwidth type is not available on the list, select Custom.
Download Bandwidth	Enter the value to customize download bandwidth.
Upload Bandwidth	Enter the value to customize upload bandwidth.
Reserved Buffering Bandwidth	Enter the value to provide bandwidth buffer.

3. Advanced Setting Example

A user subscribed 10M/2Mbps bandwidth from ISP. After performing some speed test, the user found that the actual bandwidth is about 1135KByte/sec downloading and 200KByte/s uploading. We change the dimension in Kbps as follows,

Download Speed: 1135KB/s x 8 = 9080Kbp/s

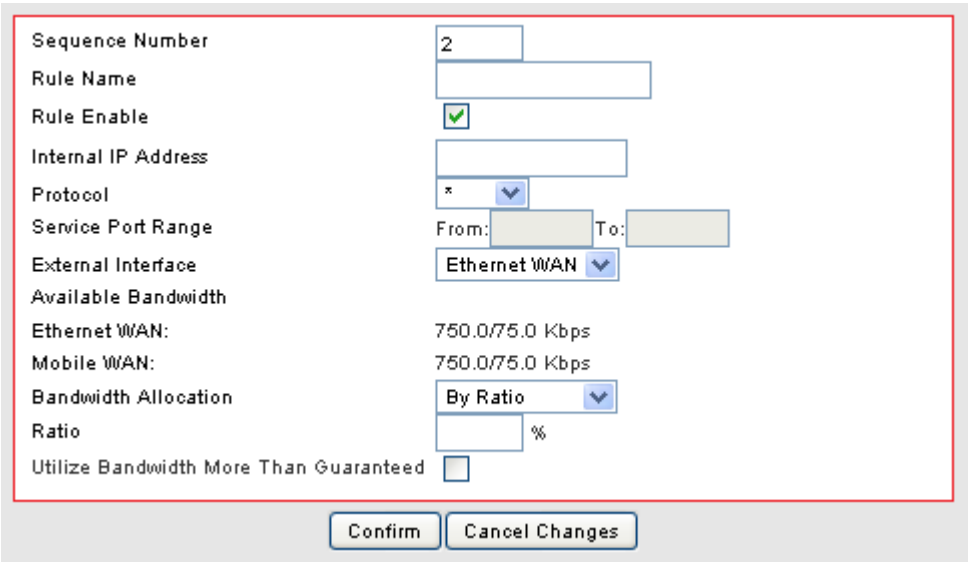
Upload Speed: 200KB/s x 8 = 1600Kbp/s

The settings can be done as below,

Bandwidth Type (Download/Upload)	Select custom。
Download Bandwidth	Enter the value to 9080。
Upload Bandwidth	Enter the value to 1600。
Reserved Buffering Bandwidth	User can firstly set the value about 10% and adjust this value later. If your network is very stable, you could lower this value.

9.1.2 Add SBM Rules

1. Click on [Add] tab. You will see the following screen.



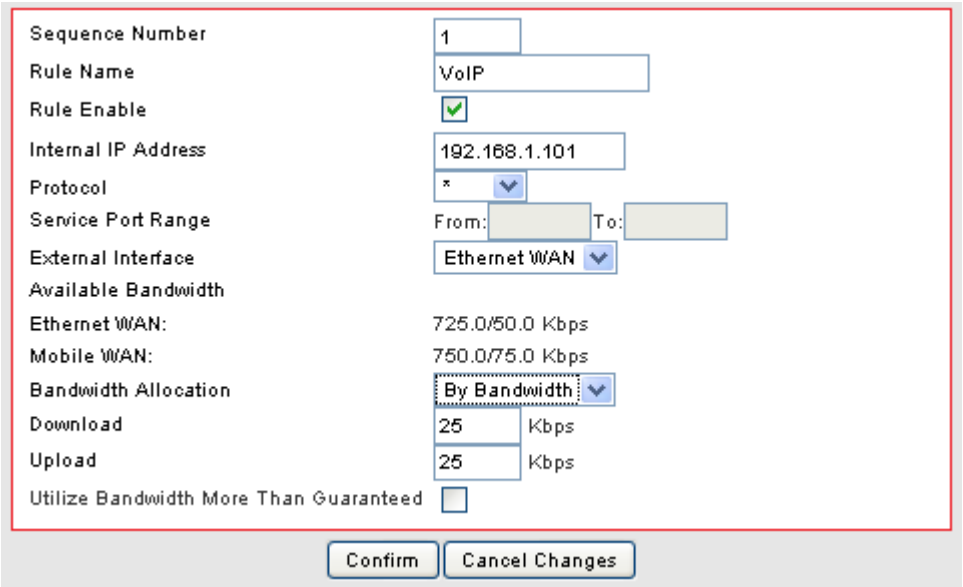
2. Configure [Add SBM] Settings following the instructions below.

Sequence Number	This defines the sequence of the SBM rules. If a packet fits the conditions set by the SBM rules, the packet will then be sorted according to the first SBM rule from the top of the list.
Rule Name	Name of the SBM rule.
Rule Enable	Enable/Disable this SBM rule
Internal IP	Set up the internal IP for this SBM rule.
Protocol	Set up the protocol (TCP or UDP) for the ACL to be enabled.

External Interface	Please select which External Interface (WAN1 or WAN2) you want a packet to go through, IF the packet fits the condition of this SBM rule.
Service Port Range	Set up the Service Port Range (e.g., HTTP is TCP/80) for the SBM to be enabled.
Bandwidth Allocation	By Ratio or By Bandwidth
Ratio	The ratio of the whole bandwidth according to the External Interface.
Download	Enter the reserved download bandwidth.
Upload	Enter the reserved upload bandwidth.
Utilize Bandwidth More than Guaranteed	Check this box if you wish to allow the traffic confirming this SBM rule to be able to utilize the whole bandwidth when the bandwidth is idle.

3. Advanced Setting Example1

If a user needs to reverse some bandwidth for a specified application, such as VoIP, one can have the following configuration to reserve a 25Kbps/25Kbps bandwidth for VoIP application.



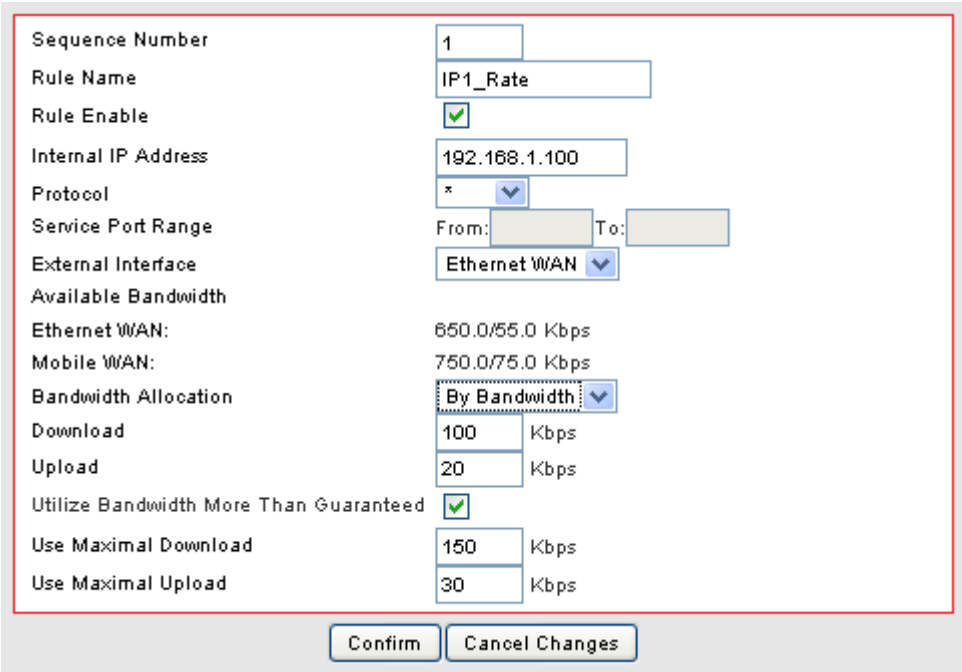
Rule Name	VoIP
Rule Enable	Check the box to enable this rule
Internal IP Address	Enter the IP address of the VoIP machine
Protocol	Select * will apply this rule for both TCP and UDP protocols
External Interface	Choose the WAN interface you want to use
Service Port Range	Enter the service port number that used by VoIP
Bandwidth Allocation	Allocating the bandwidth by fixed value assignment or ratio

Download	Enter the reserved download rate to 25 Kbps
Upload	Enter the reserved upload rate to 25 Kbps
Utilize Bandwidth More Than Guaranteed	Uncheck this box to reserve a fixed rate for this application; You may also check this box allowing this application use any free available bandwidth when it consumes more bandwidth.

4. Advanced Setting Example 2

In the case users need to guarantee a PC or a network device for a specified bandwidth and allow the user to user rest bandwidth up to some values, one may follow the settings as below.

In this case, the PC with IP address-192.168.10.100 will be guaranteed for 100Kbps/20Kbps bandwidth. Additionally, this PC can use up to 150Kbps/30Kbps if there is still any free bandwidth existed.



Rule Name	IP1_Rate
Rule Enable	Check this box to enable this rule
Internal IP Address	Enter the IP address this rule to be applied to.
Protocol	* (Applied to both TCP and UDP)
External Interface	Select the external WAN Interface to be applied to.
Service Port Range	Applied to all port range if left this field blank
Bandwidth Allocation	Allocating the bandwidth by fixed value assignment or ratio
Download	Enter the download guaranteed value to 100 Kbps。
Upload	Enter the upload guaranteed value to 25 Kbps。

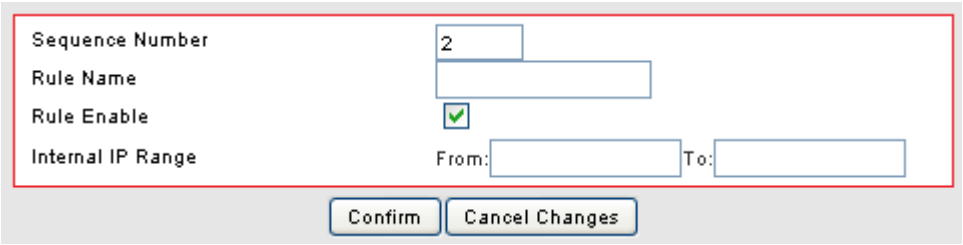
Utilize Bandwidth More Than Guaranteed	Check this box to allow the usage of free bandwidth
Use Maximal Download	Enter the limited download value to 150Kbps
Use Maximal Upload	Enter the limited upload value to 30Kbps

9.1.3 Add DBM Rule

It is very simple to set-up a DBM rule, users only need to set the IPs to be controlled in the DBM IP ranges.

After assignment of the DBM IPs, the ZyXEL VFG6005 Series VPN Firewall Gateway will dynamically control the bandwidth by equality and priority methods

1. Click on [Add] tab. You will see the following screen.

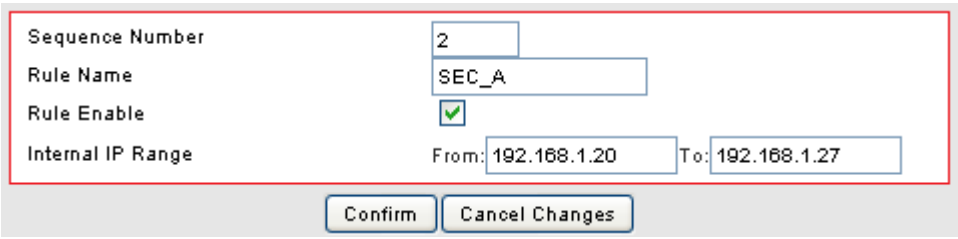


2. Configure [Add DBM] Settings following the instructions below

Sequence Number	This defines the sequence of the DBM rules.
Rule Name	Name of the DBM rule.
Rule Enable	Enable/Disable this DBM rule
Internal IP Range	Set up the internal IP range for this DBM rule.

3. DBM Setting Example

The maximum DBM IPs is 8 in the VFG6005 Series. The user may set the DHCP releasing range from 192.168.1.20 to 192.168.1.27 and set those IP as DBM IP accordingly. In this manner, all user access through this router will be controlled by DBM system without any other complicated settings.

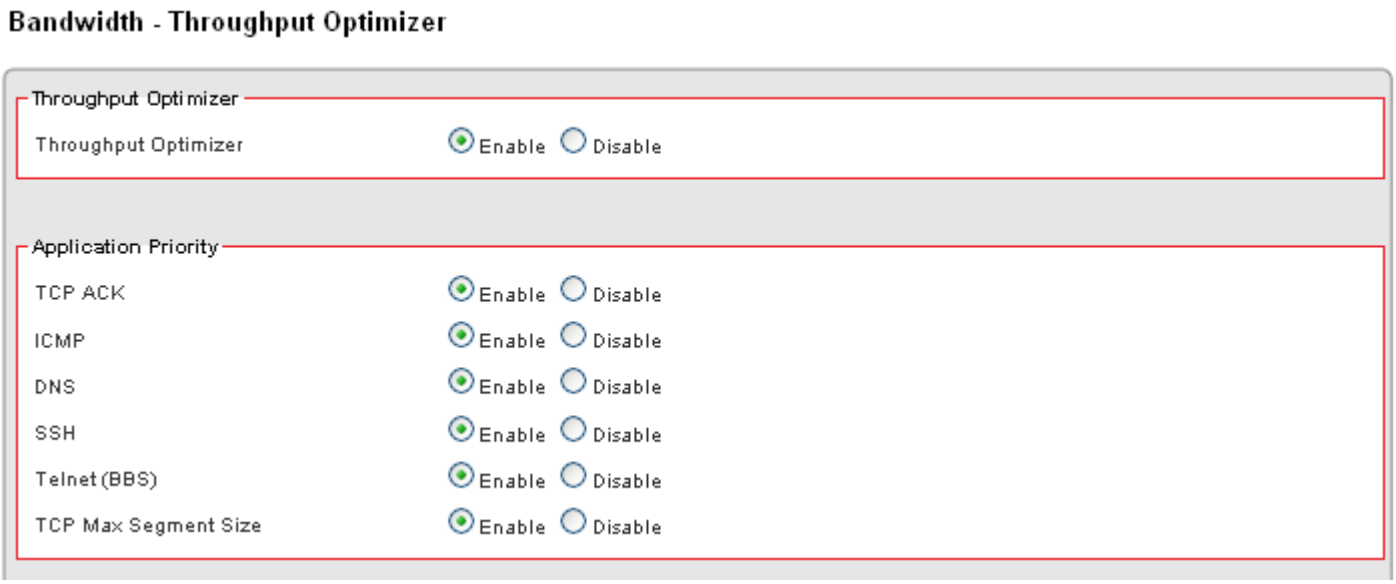


9.2 THROUGHPUT OPTIMIZER

ZyXEL's VFG6005 Series VPN Firewall Gateway built in Bandwidth Management transmits the important packets in high priority to optimize the network utilization. You can specify the types of packets for high priority.

1. Click on [Bandwidth] – [Throughput Optimizer] tab. You will see the following screen.

Please do not change the parameters unless you wish to customize it by yourself.



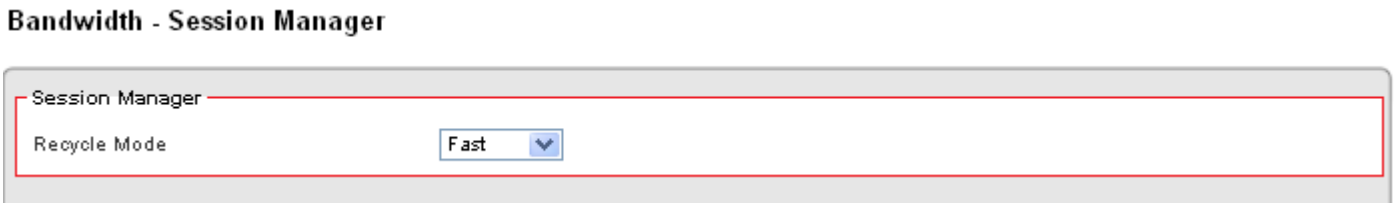
2. Configure Throughput Optimizer Settings following the instructions below

TCP ACK	Select Enable/Disable to enable/disable TCP ACK priority
ICMP	Select Enable/Disable to enable/disable ICMP priority
DNS	Select Enable/Disable to enable/disable DNS priority
SSH	Select Enable/Disable to enable/disable SSH priority
Telnet (BBS)	Select Enable/Disable to enable/disable Telnet (BBS) priority
TCP Max Segment Size	Select Enable/Disable to enable/disable TCP Max Segment Size

9.3 SESSION MANAGER

Session manager will automatically recycle old/dead sessions to get better connection efficiency. Users can choose the recycle rate to optimize the connection efficiency especially during P2P downloads. Setting to FAST is recommended.

1. Click on [Bandwidth] – [Session Manager] tab. You will see the following screen.



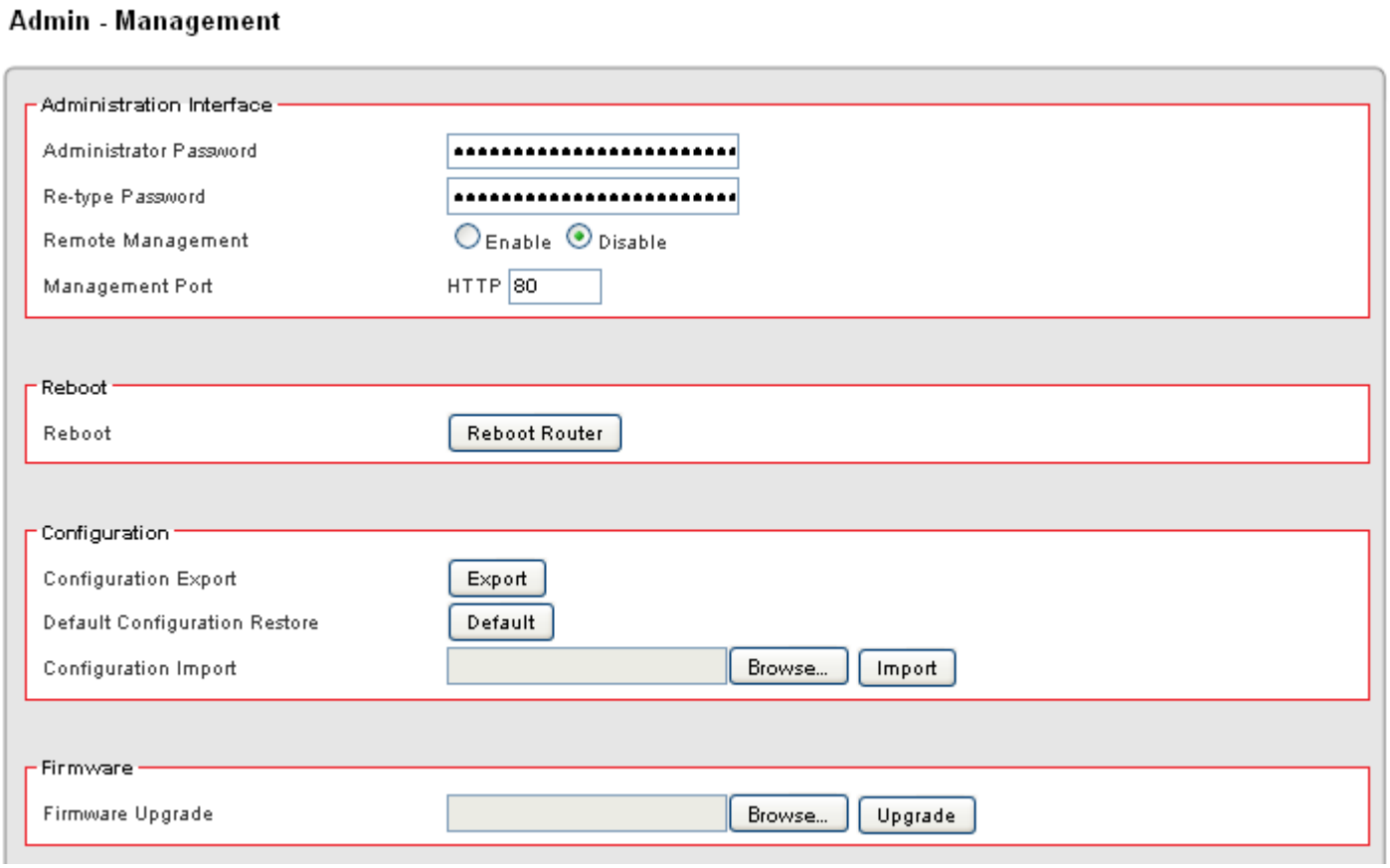
2. Configure [Session Manager] Settings following the instructions below

Recycle Mode	Select Fast/Regular/Slow recycle rate

CHAPTER10 ADMIN

10.1 MANAGEMENT

1. Click on [Admin] – [Management] tab. You will see the following screen.



2. Configure [Administration Interface] Settings based on the instructions listed below.

Administrator Password	Maximum input is 36 alphanumeric characters (case sensitive) * Please change the administrator's password if the remote management is enabled. Otherwise, a malicious user can access the management interface. This user can then have the ability to change the settings and interrupt your network access.
Re-type Password	Enter the password again to confirm.
Remote Management	Select Enable to enable Remote Management. Select Disable to disable Remote Management If the remote management is enabled, users who are not in the LAN can connect to the ZyXEL VFG6005 Series VPN Firewall Gateway and configure it from the Internet.
Management Port	HTTP port which users can connect to. (default port is 80)

3. Configure [Configuration] Settings based on the instructions listed below

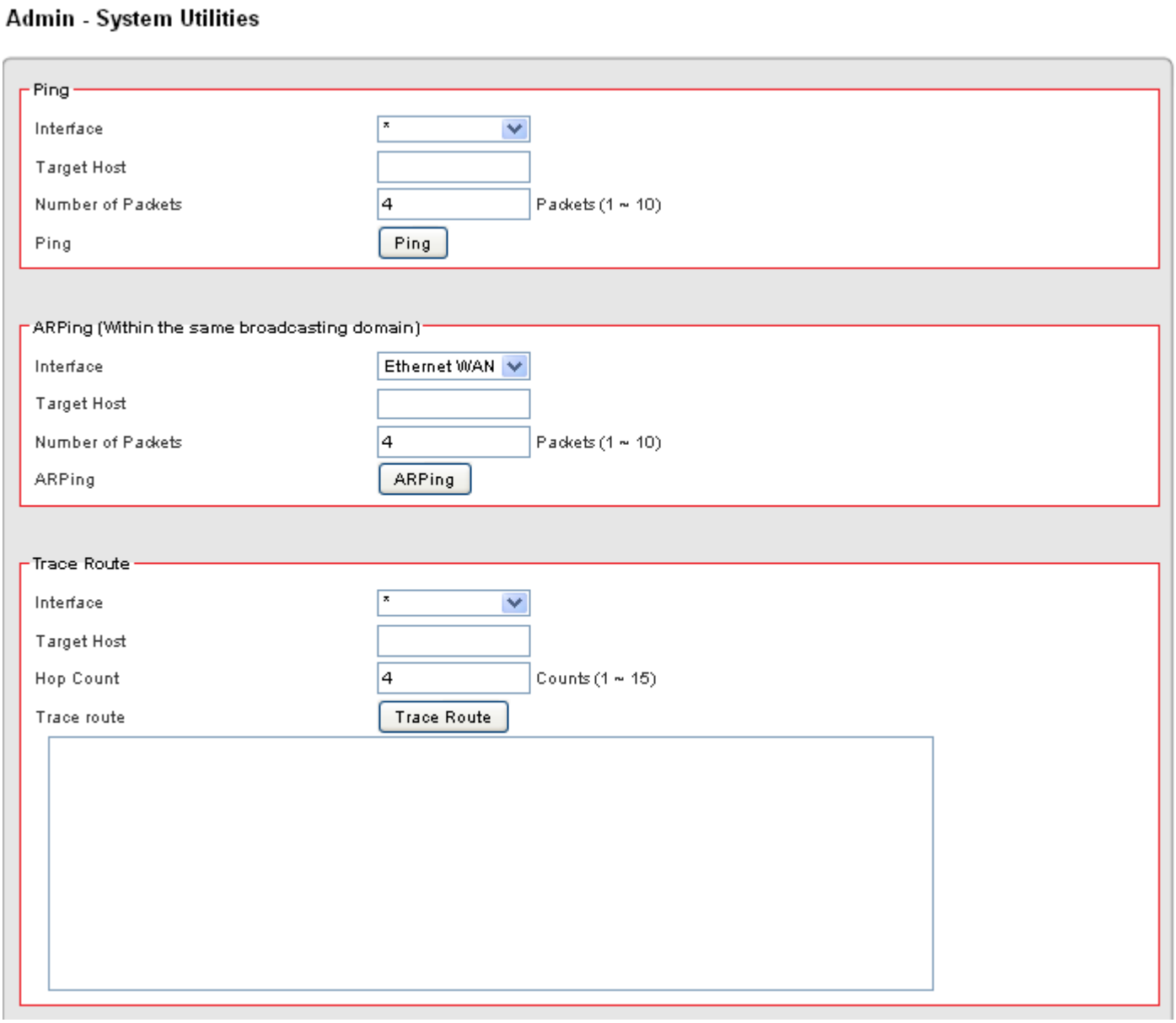
Configuration Export	Click Export to save your current configuration settings in a file.
Default Configuration Restore	Click Default to recover the default system settings.
Configuration Import	Click Browse and Import to load previous configuration settings.

4. Configure [Firmware] Settings based on the instructions listed below

Firmware Upgrade	Click Browse and Upgrade to upgrade the firmware.

10.2 SYSTEM UTILITIES

1. Click on [Admin] – [System Utilities] tab. You will see the following screen.



2. Using the [ping] tool based on the instructions listed below

Interface	Select the interface that you want to use to ping from, i.e. LAN, WAN.
Target Host	Enter the IP address to ping to
Number of Packets	Specify the number of the ICMP packets to send out
Ping	Press the tab to start the “ping” actions

3. Using the [ARPing] tool based on the instructions listed below

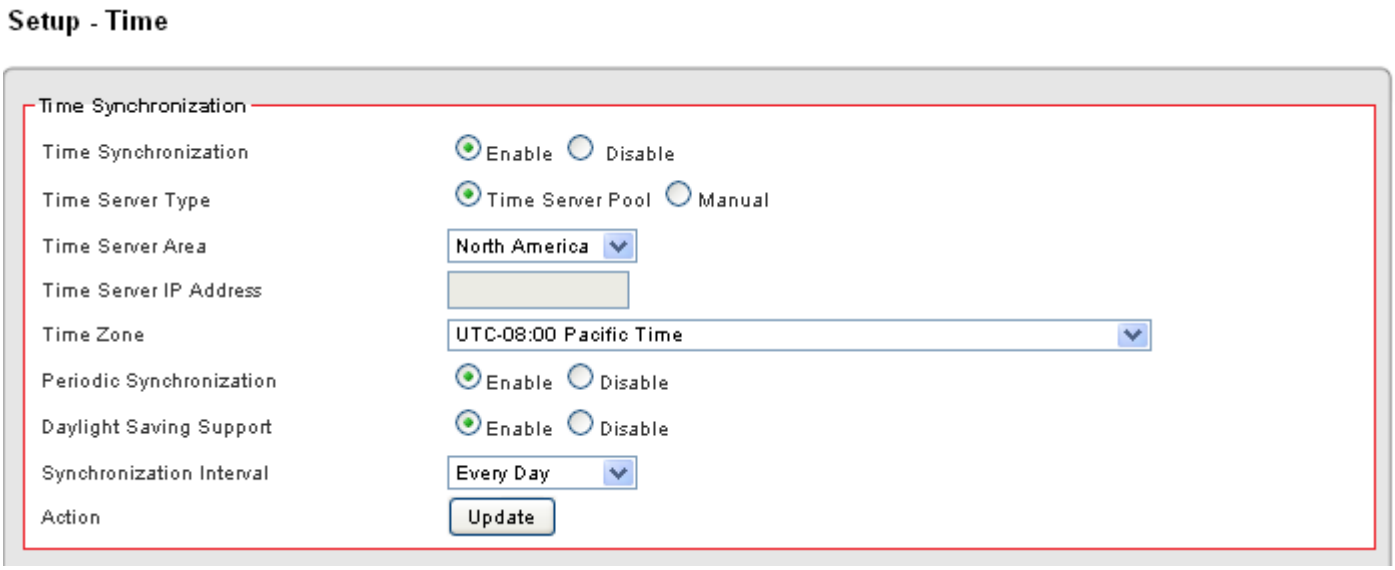
Interface	Select the interface that use to ARPing to, i.e. LAN, WAN.
Target Host	Enter the MAC address to ARPing to
Number of Packets	Specify the number of the ARP request packets to send out
ARPing	Press the tab to start the “ARPing” actions

4. Using the [Trace Route] tool based on the instructions listed below

Interface	Select the interface that use to ARPing to, i.e. WAN1, WAN2.
Target Host	Enter the destination IP address / domain name to trace
Hop Count	Specify the Hop number you need to trace
Trace route	Press the tab to start the “Trace Route” actions

10.3 TIME SETUP

5. Click on [Admin] – [Time] tab. You will see the following screen.



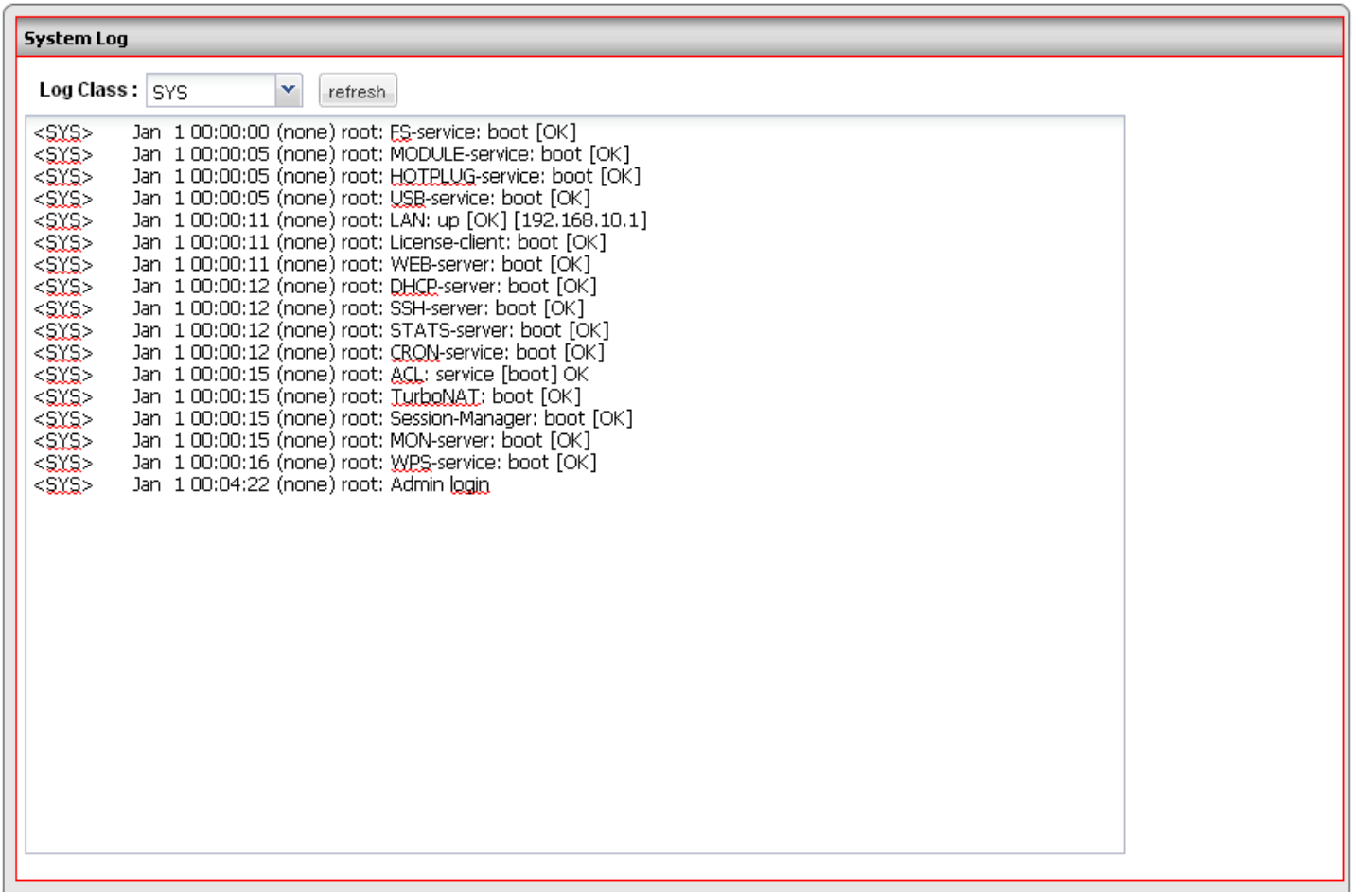
6. Configure [Time] Settings based on the instructions listed below

Time Synchronization	Select Enable/Disable to enable/disable Time Synchronization
Time Server Type	Select Time Server Pool or Manual.
Time Server Area	Select Time Server according to your location. You can choose from Automatic, Asia, Europe, North America, South America, or Africa.
Time Zone	Select Time Zone according to your location.
Periodic Synchronization	Select Enable/Disable to enable/disable Periodic Synchronization
Daylight Savings Support	Select Enable/Disable to enable/disable Daylight Savings Time.
Synchronization Interval	Select from Every Hour, Every 6 Hours, Every 12 Hours, Every Day, and Every Week.
Action	Click update to update the Time Settings immediately.

10.4 LOG

1. Click on [Admin] – [Log] tab. You will see the following screen.

Admin - Log



CHAPTER11 STATUS

You can access and view all the system information regarding The ZyXEL VFG6005 Series VPN Firewall Gateway from here.

11.1 ROUTER INFORMATION

1. Click on [Status] – [Router] tab. You will see the following screen.

Status - Router

Router Information

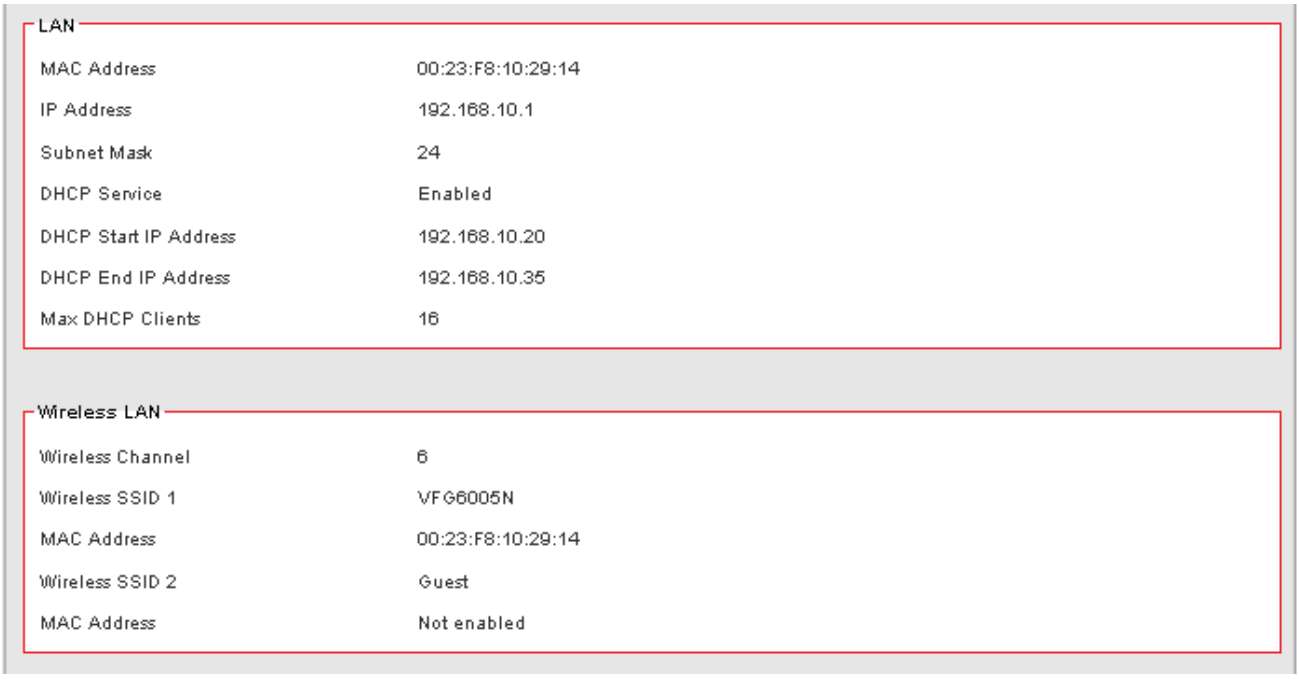
Model Name	ZyXEL VFG6005N
Firmware Version	2.04_VFG.0_b8_20110210
Current Time	Mon, 14 Feb 2011 10:54:05
Running Time	2 days, 18 hours, 43 mins

Ethernet WAN

Connection Status	Not Connected
MAC Address	00:23:F8:10:29:16
Connection Type	dhcp
IP Address	
Subnet Mask	
Gateway	
Download	0 B/s
Upload	172 B/s

Mobile WAN

Connection Status	Connected
MAC Address	00:00:00:00:00:00
Connection Type	wwan
IP Address	184.233.98.186
Subnet Mask	32
Gateway	68.28.49.69
Download	167 B/s
Upload	208 B/s
Modem Brand	Auto
Modem Model	Auto
Service Provider	



2. Router Information

Model Name	Product model name is shown.
Firmware Version	The firmware version this device is running.
Current Time	Current system time
Running Time	The period of time The ZyXEL VFG6005 Series VPN Firewall Gateway has been running.

3. WAN Ethernet

Connection Status	Connected / Not Connected
MAC Address	MAC Address
Connection Type	The current connection type (PPPoE, Static IP, and DHCP)
IP Address	WAN IP Address
Subnet Mask	Number of subnet mask.
Gateway	IP address of the gateway
Download	Download speed
Upload	Upload speed

4. WAN Mobile

Connection Status	Connected / Not Connected
Connection Type	The current connection type
IP Address	WAN IP Address
Subnet Mask	Number of subnet mask
Gateway	IP address of the gateway
Download	Download speed
Upload	Upload speed
Modem Brand	Modem brand
Modem Model	Modem model name

5. LAN Ethernet

MAC Address	MAC Address
IP Address	Internal IP Address
Subnet Mask	The number of subnet mask in the internal network
DHCP Service	DHCP service enabled or disabled
DHCP Start IP Address	DHCP Start IP address
DHCP End IP Address	DHCP End IP address
Max DHCP Clients	The maximum IP addressed which can be assigned to PCs connecting to the network

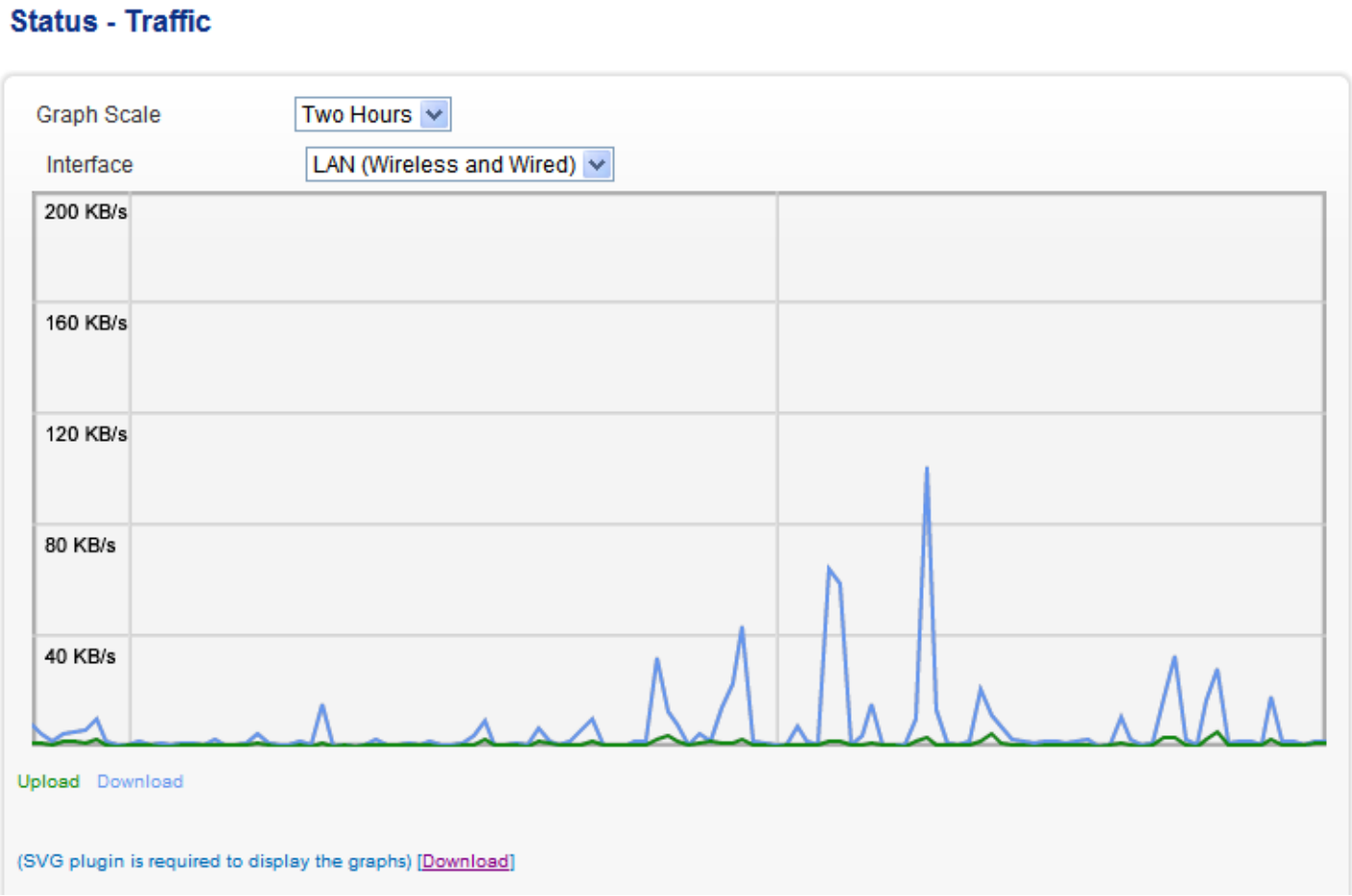
6. Wireless Network Ethernet

Wireless Channel	Wireless Channel in use (default is 6)
Wireless SSID 1	SSID 1of this Wi-Fi station
MAC Address	Shows MAC Address if enabled
Wireless SSID 2	SSID 2 of this Wi-Fi station
MAC Address	Shows MAC Address if enabled

11.2 TRAFFIC

1. Click on [Status] – [Traffic] tab, and then choose the graph scale from two hours, one day, one week, and one month. You will see the following graph.

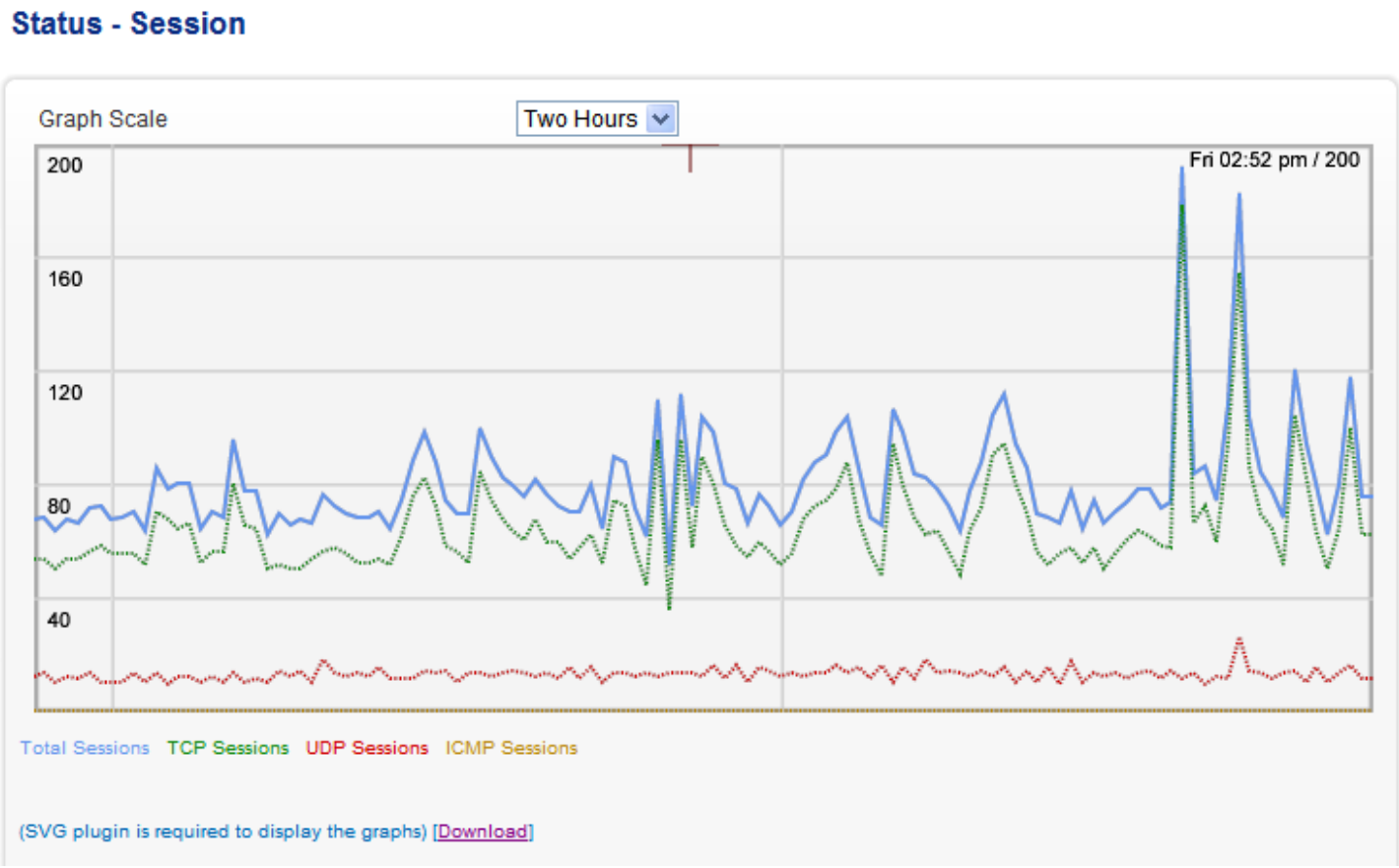
Now you can monitor your download and upload throughput.



11.3 SESSION

1. Click on [Status] – [Session] tab and choose the graph scale from two hours, one day, one week, and one month. You will now see the following graph.

TCP, UDP, ICMP, and total session information is displayed.



11.4 USER/DHCP

1. Click on [Status] – [User/DHCP] tab. You will see the following screen.

Status - User

DHCP Table (2 users)

Name	IP Address	MAC Address	Expiration Time
DAVIDN-PC	192.168.10.27	00:15:c5:5b:d7:7b	22:31:41
pikachu	192.168.10.25	00:13:20:46:8c:d0	21:33:44

Name	DHCP client name
IP Address	IP address which is assigned to this client
MAC Address	MAC address of this client
Expiration Time	The remaining time of the IP assignment

11.5 USER/ Current

1. Click on [Status] – [User/Current] tab. You will see the following screen.

Status - User

ARP Table (2 users)

IP Address	MAC Address	ARP Type
192.168.10.25	00:13:20:46:8c:d0	Dynamic
192.168.10.27	00:15:c5:5b:d7:7b	Dynamic

IP Address	IP address assigned by Static ARP matching
MAC Address	MAC address in the Static ARP matching
ARP Type	Static or dynamic

Product Specifications

The following tables summarize the VFG6005 Series hardware and firmware features.

Hardware Features	
Dimensions (W x D x H)	159 mm x 107 mm x 25 mm
Weight	225 g
Power Specification	Input: 100~240 V AC, 50~60 Hz Output: 12 V DC 1.5 A
Gigabit Ethernet ports	Auto-negotiating: 100 Mbps, 1000 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
4 Port Gigabit Switch	A combination of switch and router makes your VFG a cost-effective network solution. You can add up to four computers to the VFG without the cost of a hub when connecting to the Internet through the WAN. Add more than four computers to your LAN by using another hub or switch.
LEDs	PWR/SYS, WLAN (VFG6005N), WAN, LAN1-4
Reset Button	The reset button is built into the rear panel. Use this button to restore the VFG to its factory default settings. Press for 1 second to restart the device. Press and hold for 7 seconds or until PWR/SYS LED is blinking to restore to factory default settings.
Antenna	The VFG6005N is equipped with two 2dBi (2.4GHz) detachable antennas to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0º C ~ 40º C / 32ºF ~ 104ºF

	Humidity: 20% ~ 90%
Storage Environment	Temperature: -30º C ~ 70º C / -22ºF ~ 158ºF Humidity: 20% ~ 95%

Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.10.1 (router)
Default Subnet Mask	255.255.255.0 (24 bits)
Default Login/Password	admin/1234
DHCP Pool	192.168.10.20 to 192.168.10.35
Wireless Interface	Wireless LAN
Default Wireless SSID	VFG6005N
Default Wireless DHCP Pool Size	Wireless LAN: Same as LAN (16 from 192.168.10.20 to 192.168.10.35)
Device Management	Use the Web Configurator to easily configure the rich range of features on the VFG.
Wireless Functionality	Allows IEEE 802.11b/g and/or IEEE 802.11n wireless clients to connect to the VFG wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The VFG may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the VFG. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the VFG's configuration and put it back on the VFG later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the VFG for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked 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 for example.
Content Filter	The VFG blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can use category-based content filtering via OpenDNS that allows your VFG to check web sites against an external database.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether you can access the HTTP Web GUI remotely from a computer on the Internet.
Time and Date	Get the current time and date from an external server when you turn on your VFG. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host	Use this feature to have the VFG assign IP addresses, an IP default

Configuration Protocol)	gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
Logging	Use logs for troubleshooting. You can view logs in the Web Configurator.
PPPoE	PPPoE mimics a dial-up Internet access connection.
Universal Plug and Play (UPnP)	The VFG can communicate with other UPnP enabled devices in a network.

Appendices and Index

Appendix A

Pop-up Windows, JavaScripts and Java Permissions

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (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

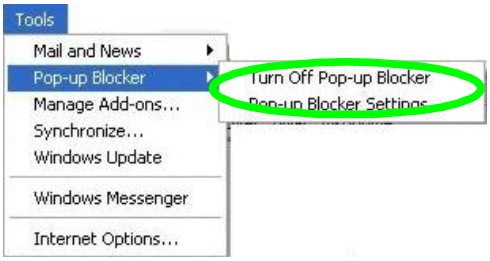
You may have to disable pop-up blocking to log into your device.

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 130 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.

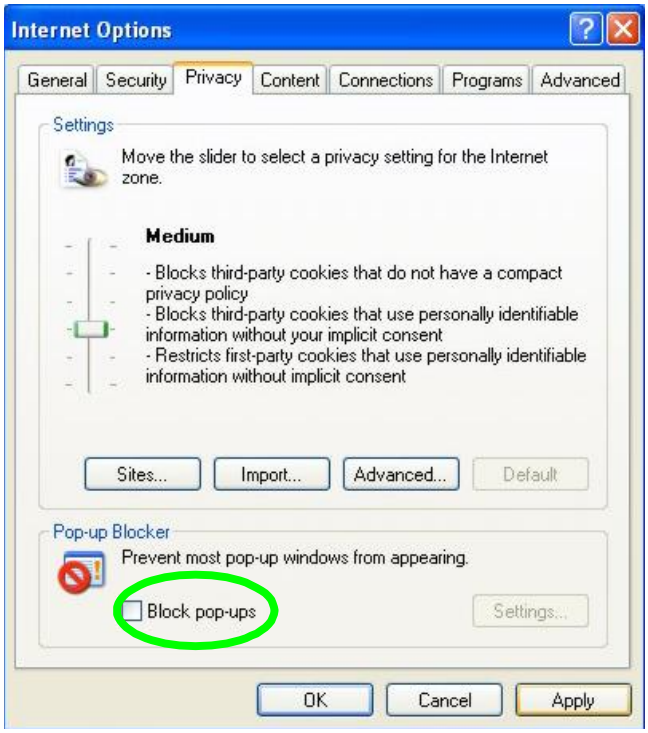


Figure 131 Internet Options: Privacy

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.

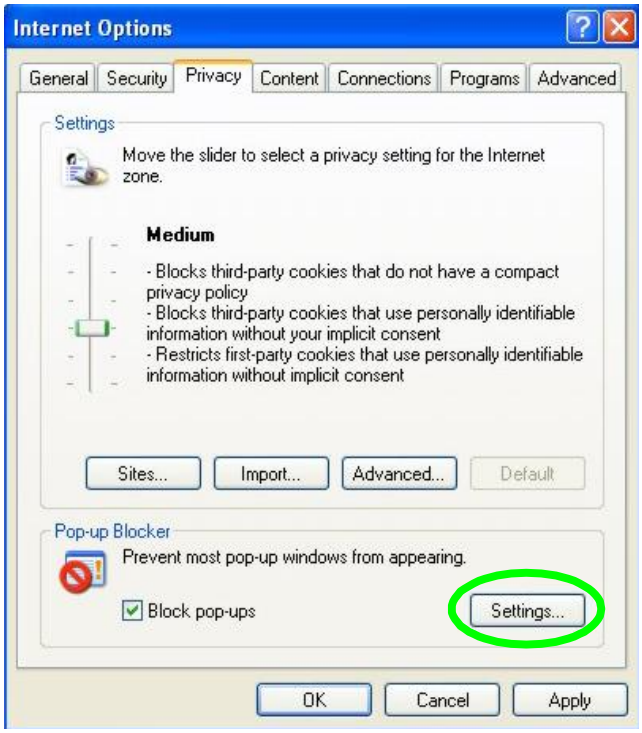


Figure 132 Internet Options: Privacy

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 133 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

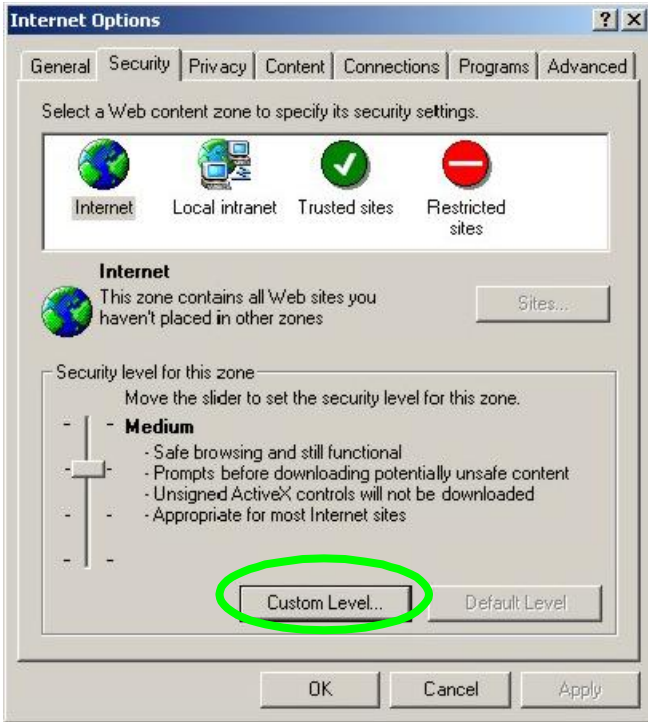
6 Click **Apply** to save this setting.

JavaScripts

If pages of the Web Configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 134 Internet Options: Security



2 Click the **Custom Level...** button.

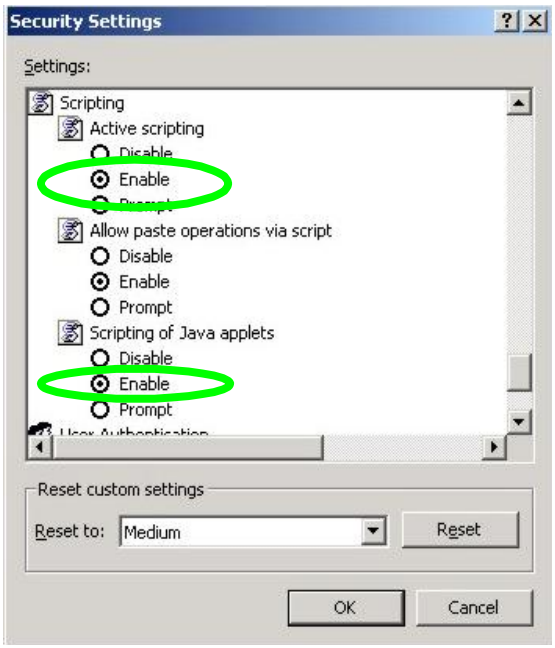
3 Scroll down to **Scripting**.

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.

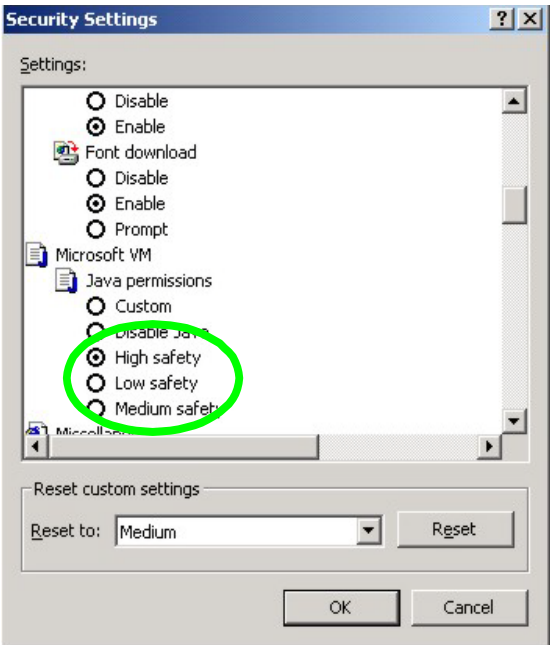
Figure 135 Security Settings - Java Scripting



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 136 Security Settings – Java



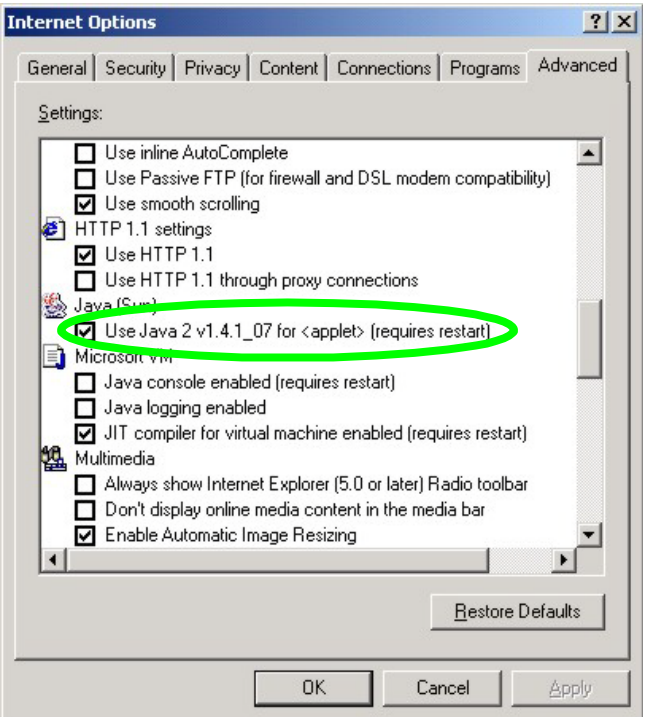
JAVA (Sun)

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 137 Java (Sun)


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
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
Use Java 2 v1.4.1_07 for <applet> (requires restart)
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
Restore Defaults
OK
Cancel
Apply

Appendix 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.

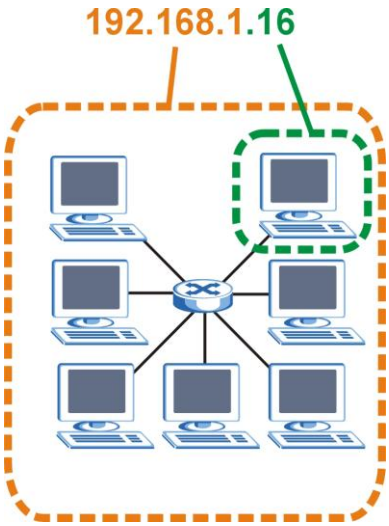
Structure

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 138 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).

Subnet Mask - Identifying Network Number				
	1ST OCTET:	**2ND OCTET:**	**3RD OCTET:**	**4TH OCTET**

	(192)	(168)	(1)	(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

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:

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.

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

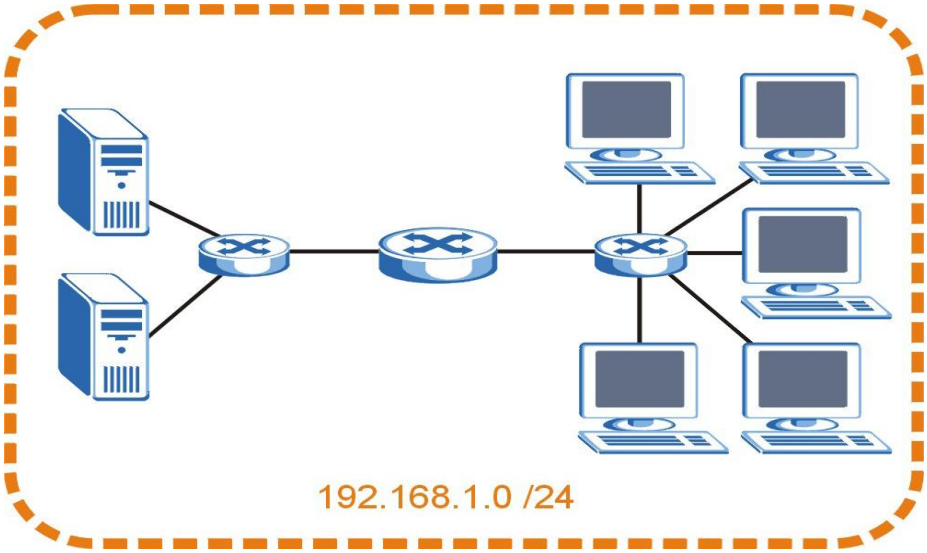
Subnetting

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 139 Subnetting Example: Before



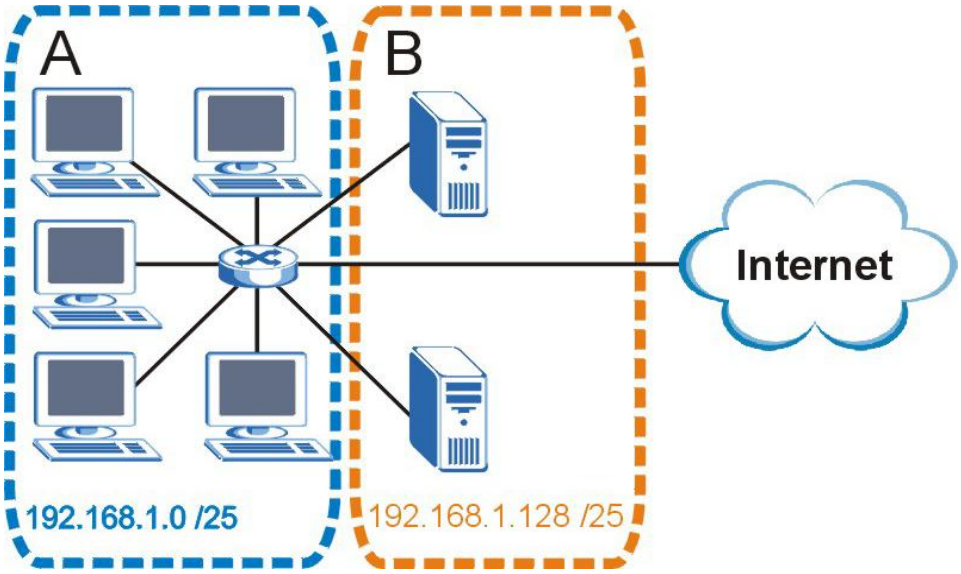
Subnetting

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 140 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).

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
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	

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	

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:	Highest Host ID: 192.168.1.190	

192.168.1.191	

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.

Eight Subnets				
SUBNET	**SUBNET ADDRESS**	**FIRST ADDRESS**	**LAST ADDRESS**	**BROADCAST ADDRESS**

1	0	1	30	31
2	32	33	62	63
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.

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.

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 VFG.

Once you have decided on the network number, pick an IP address for your VFG that is easy to remember (for instance, 192.168.10.1) 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 VFG 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 VFG 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.*

Appendix C

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, 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 Prestige’s LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

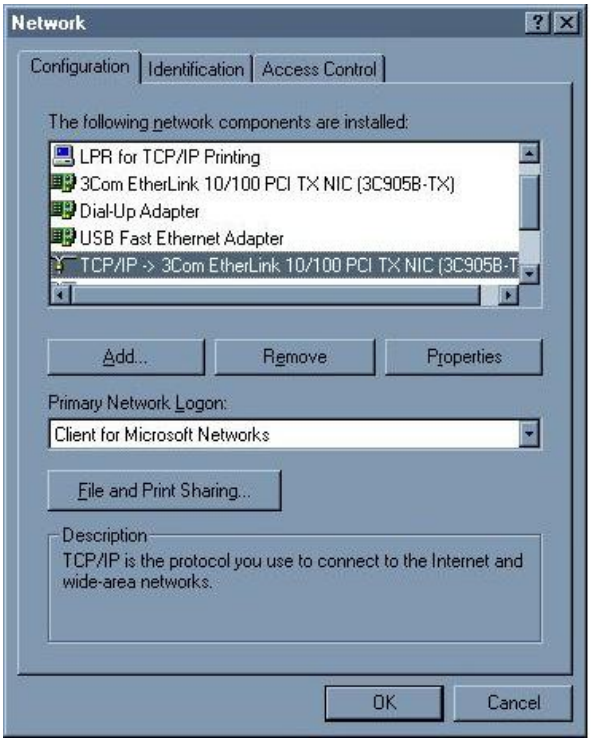


Figure 141 WIndows 95/98/Me: Network: Configuration

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.

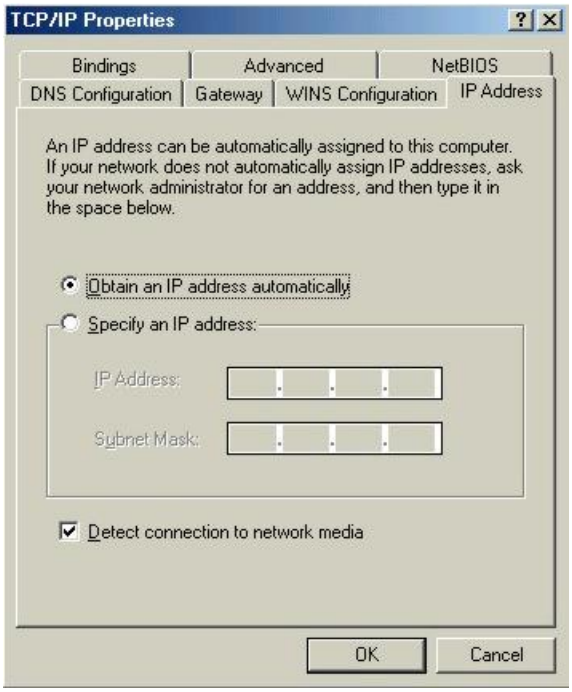
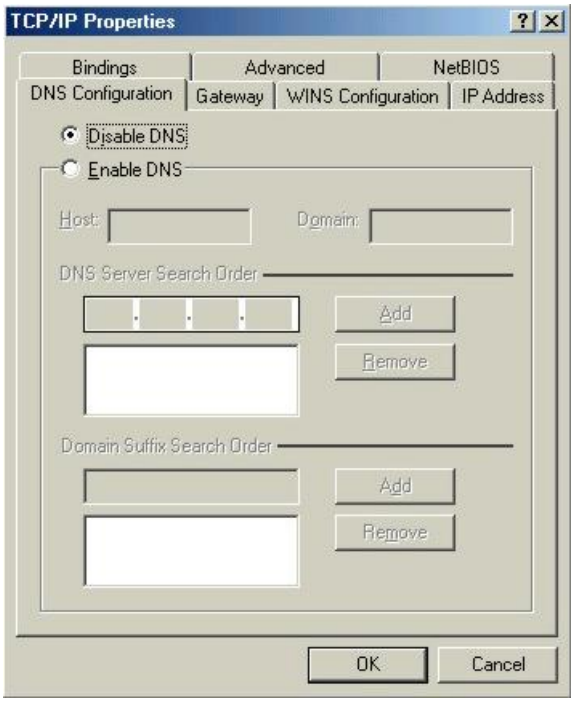


Figure 142 Windows 95/98/Me: TCP/IP Properties: IP Address

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 143 Windows 95/98/Me: TCP/IP Properties: DNS



Configuration

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 router 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**.

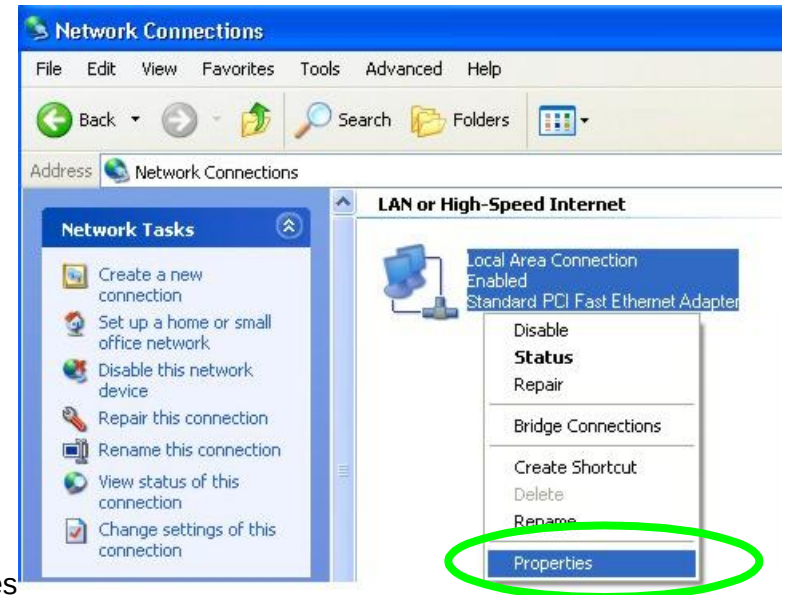
Figure 144 Windows XP: Start Menu

2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 145 Windows XP: Control Panel

3 Right-click **Local Area Connection** and then click **Properties**.

Figure 146 Windows XP: Control Panel: Network Connections:



Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

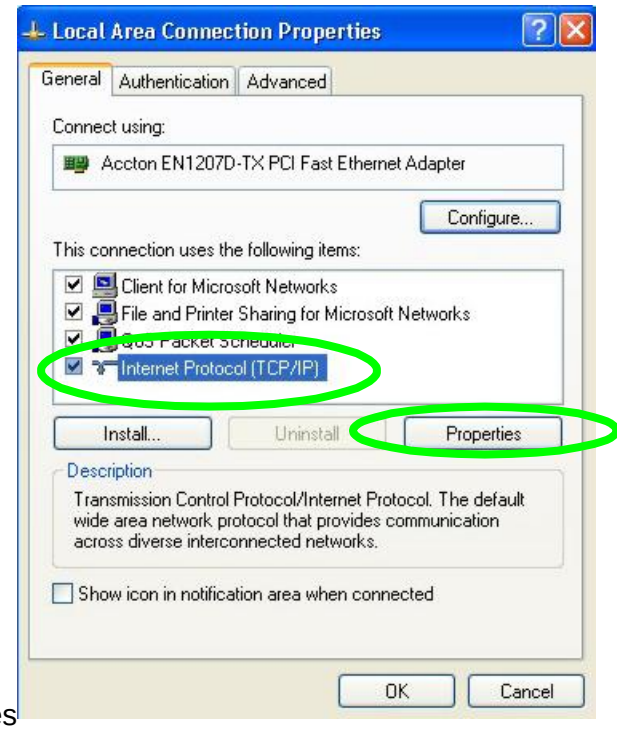
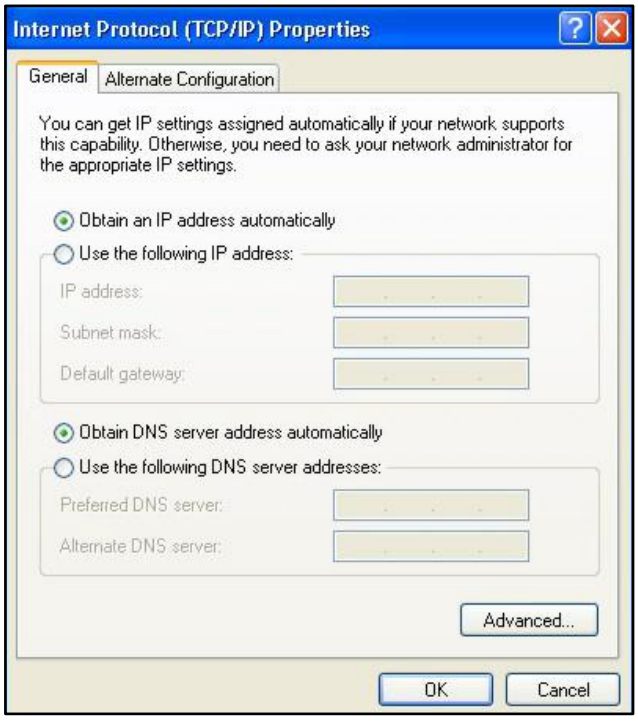


Figure 147 Windows XP: Local Area Connection Properties

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 148 Windows XP: Internet Protocol (TCP/IP)

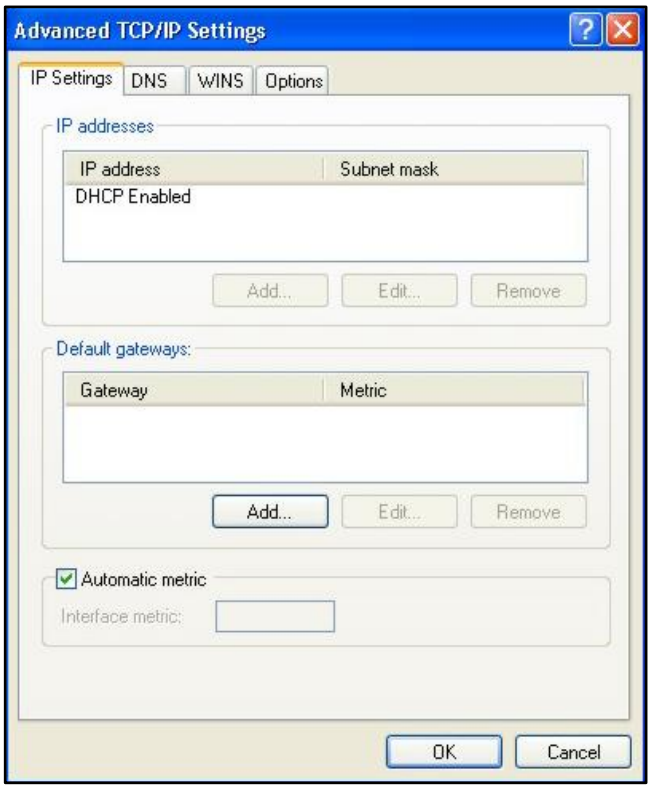
Properties 

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 149 Windows XP: Advanced TCP/IP



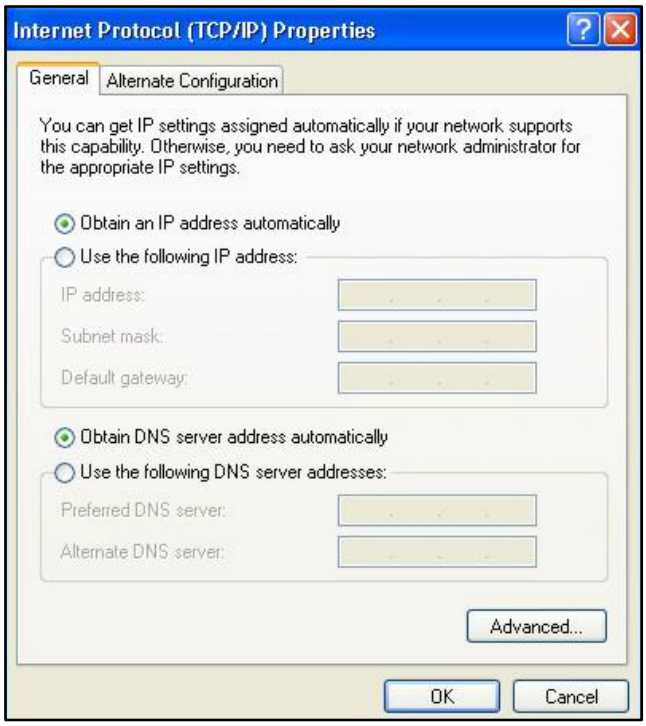
Properties

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 150 Windows XP: Internet Protocol (TCP/IP)



Properties

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 router and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

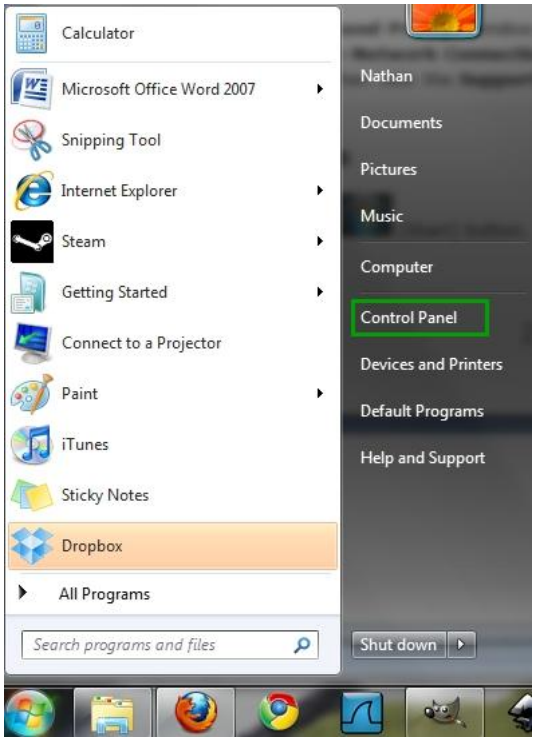
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows 7/Vista

1 Click on the  (**Start**) button.

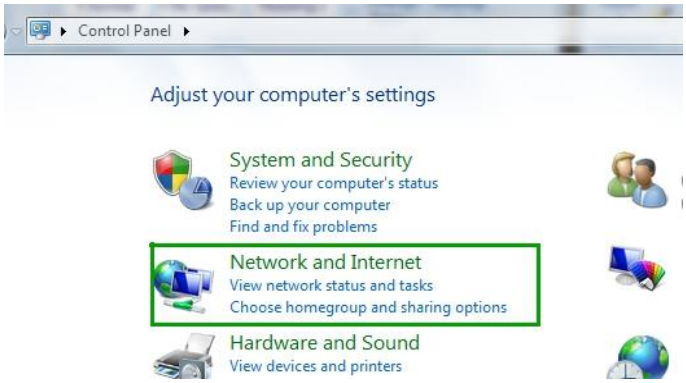
2 Click on **Control Panel.**

Figure 151 Windows 7/Vista



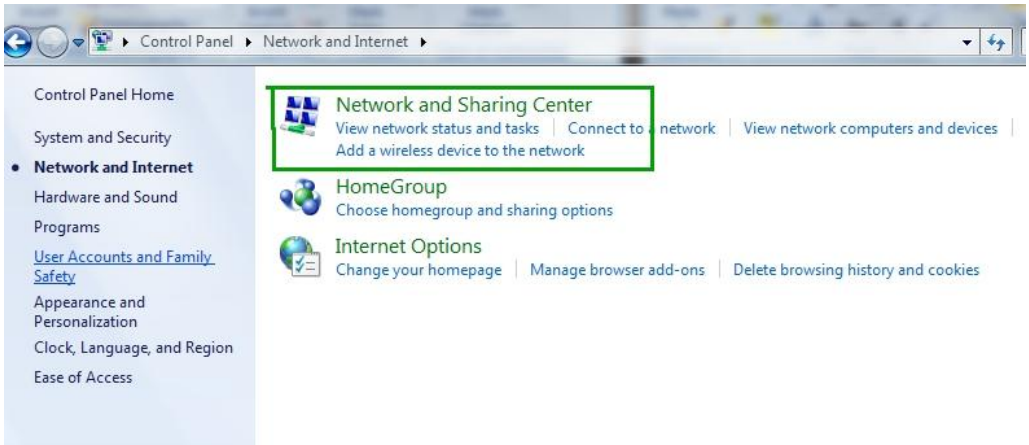
3 Click on **Network and Internet**.

Figure 152 Windows 7/Vista



4 Click on **Network and Sharing Center**

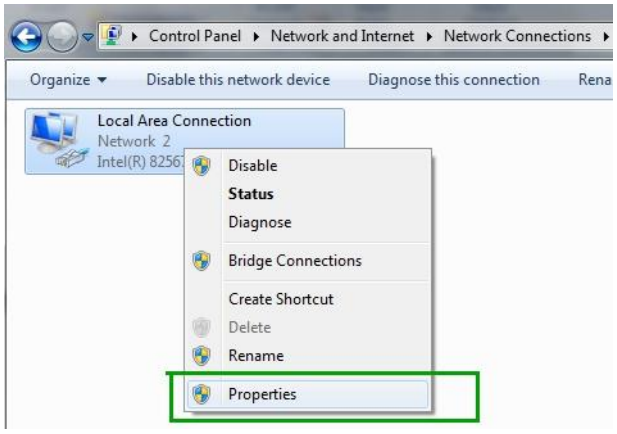
Figure 153 Windows 7/Vista



5 On the left side of the screen click on **Change Adapter Settings** (Windows 7), or **Manage Network Connections** (Vista).

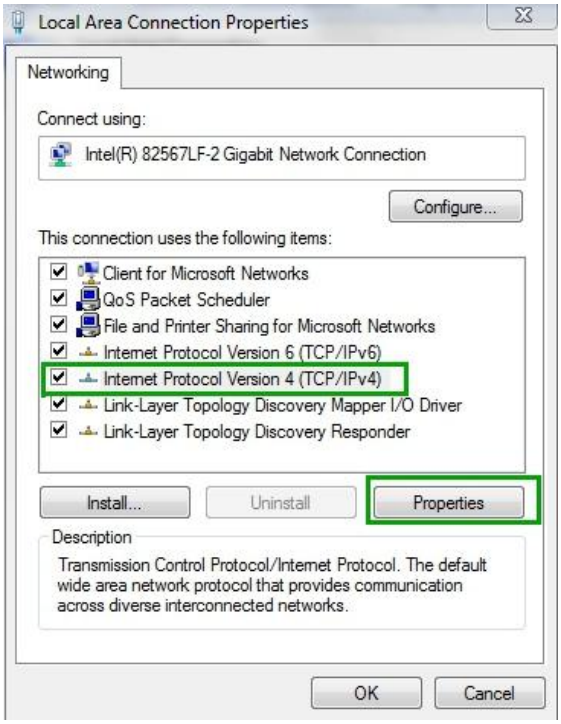
6 Right click on **Local Area Connection** and select **Properties**.

Figure 154 Windows 7/Vista



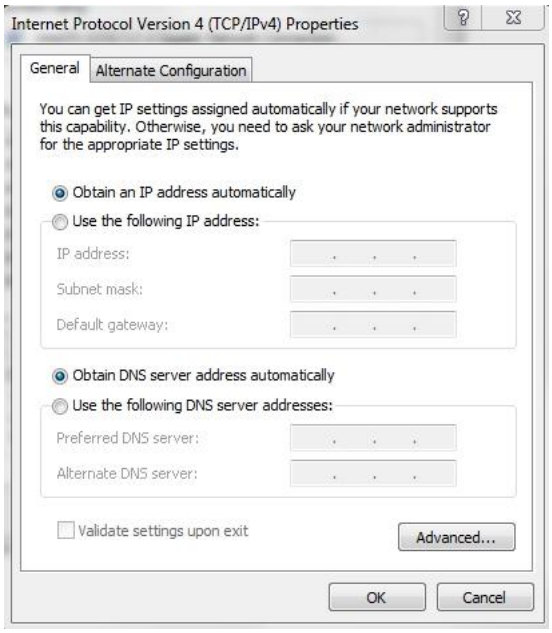
7 Highlight **Internet Protocol Version 4** and click **Properties**.

Figure 155 Windows 7/Vista



8 Select **Use the Following IP Address** and enter your IP address, Subnet Mask, and Default Gateway. Enter your DNS server address (if trying to connect to the internet) and click **OK**.

Figure 156 Windows 7/Vista



9 Click **OK** or **Close** on the Local Area Connection Properties window to apply the settings.

Macintosh OS 8/9

1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 157 Macintosh OS 8/9: Apple Menu

2 Select **Ethernet built-in** from the **Connect via** list.

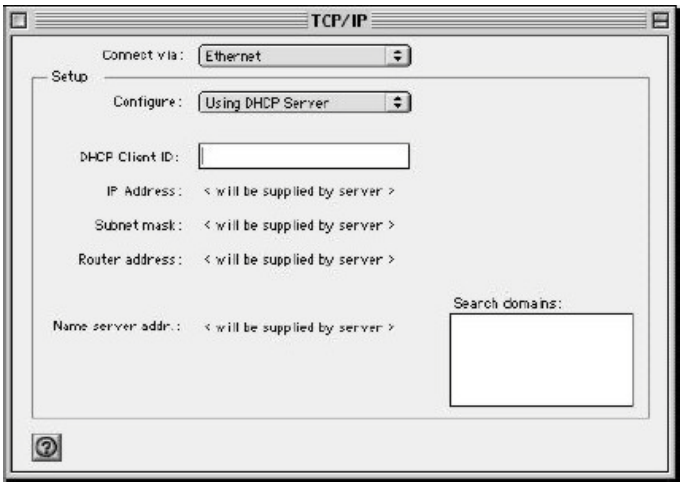


Figure 158 Macintosh OS 8/9: TCP/IP

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 Prestige 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 router and restart your computer (if prompted).

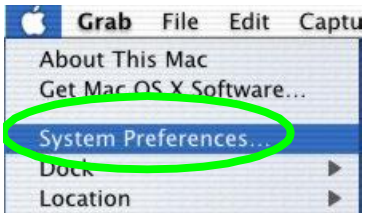
Verifying Settings

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 159 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.

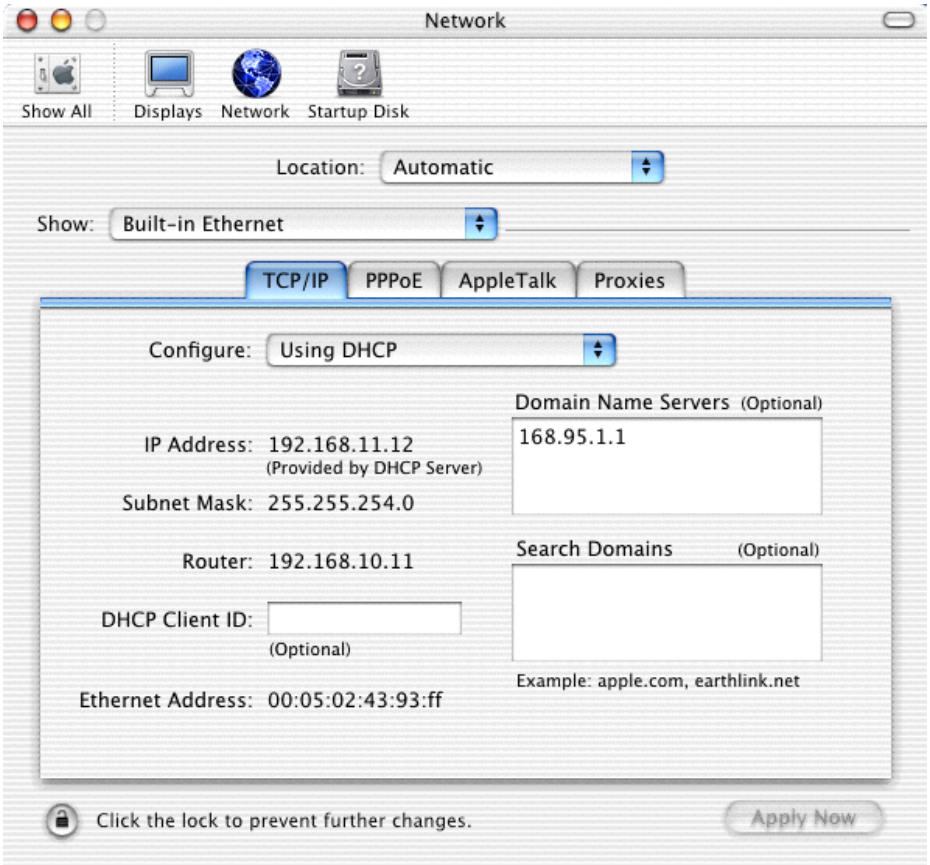


Figure 160 Macintosh OS X: Network

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 Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your router 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.

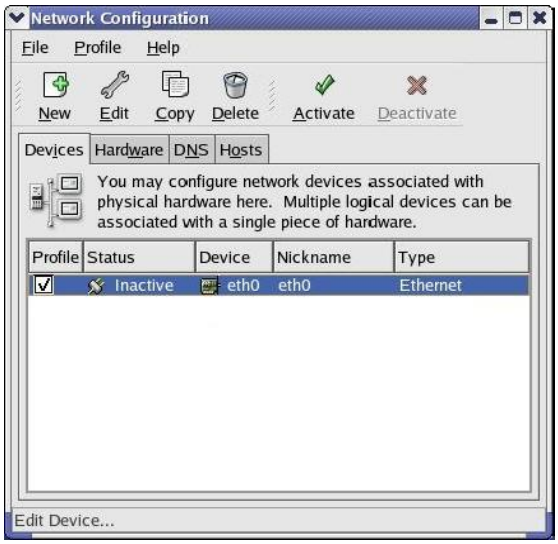
Note: Make sure you are logged in as the root administrator.

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 161 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

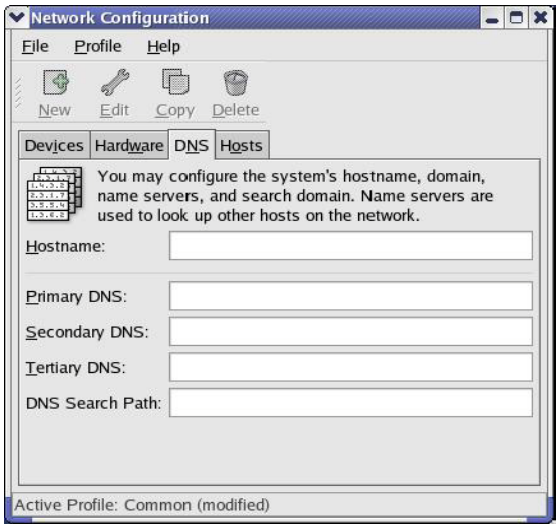
Figure 162 Red Hat 9.0: KDE: Ethernet Device: General

- 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.

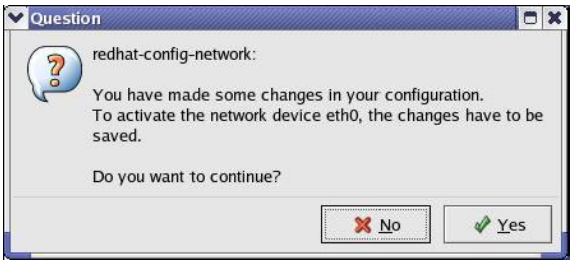
Figure 163 Red Hat 9.0: KDE: Network Configuration: DNS



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 164 Red Hat 9.0: KDE: Network Configuration: Activate



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 165 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 192.168.10.10 and the subnet mask is 255.255.255.0.

Figure 166 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.10.10
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 167 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 168 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]
```

34.1.2 Verifying Settings

Enter ifconfig in a terminal screen to check your TCP/IP properties.

Figure 169 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]#
```

Appendix D

Wireless LANs

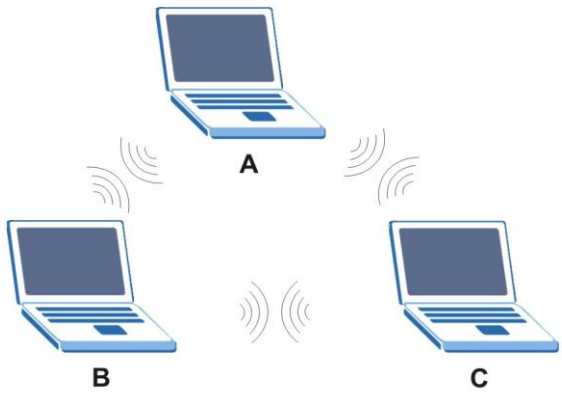
Wireless LAN Topologies

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 stations (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 170 Peer-to-Peer Communication in an Ad-hoc



Network

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

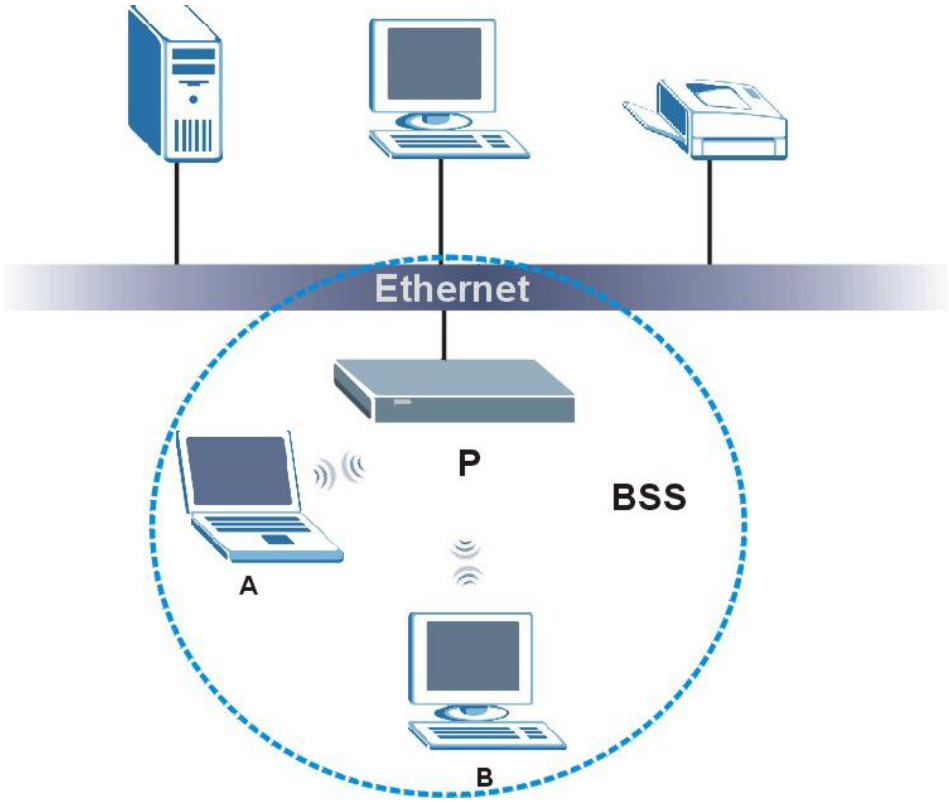


Figure 171 Basic Service Set

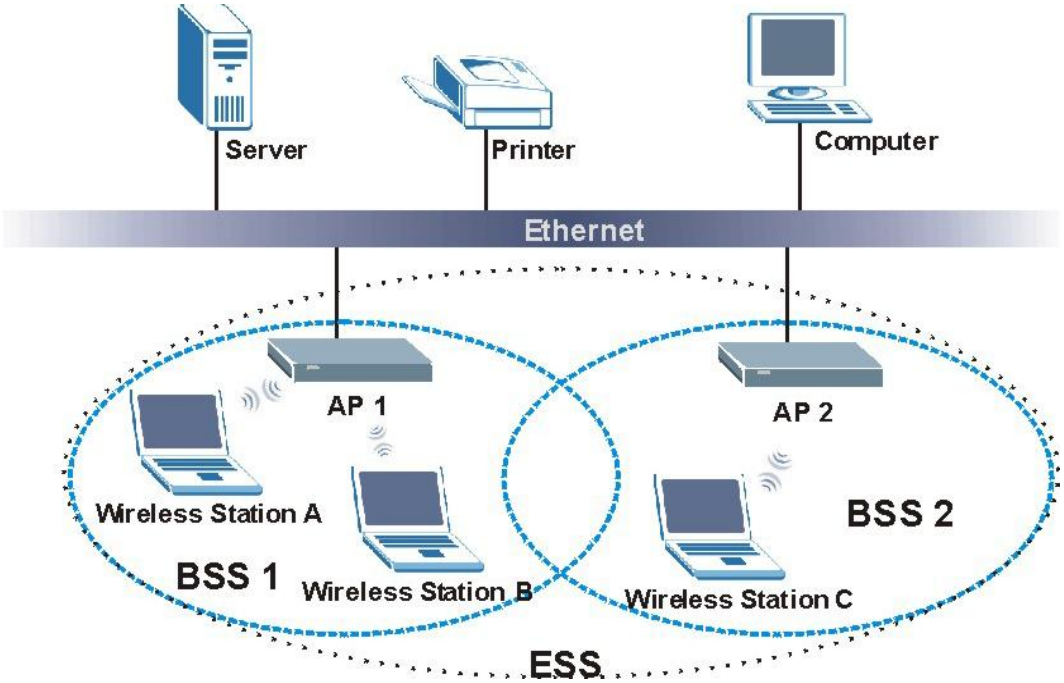
ESS

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 stations within the same ESS must have the same ESSID in order to communicate.

Figure 172 Infrastructure



WLAN

Channel

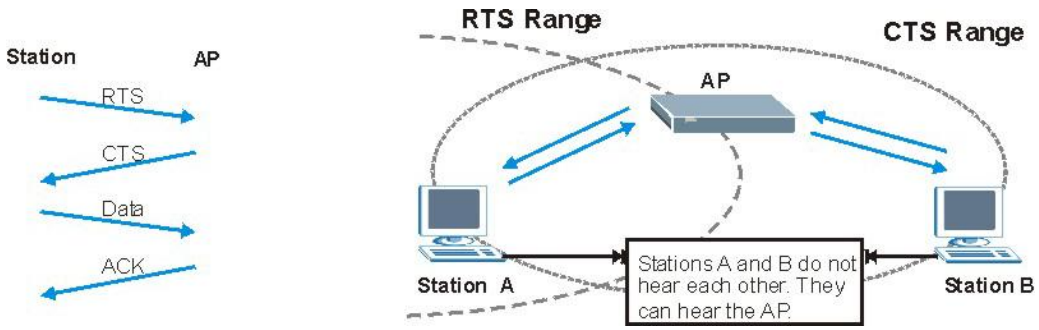
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs 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 173 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.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

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:

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)

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 stations.

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 station 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 Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station ‘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 stations 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 screen. You may still configure and store keys here, 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.

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(2)

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(2) and WEP are improved data encryption and user authentication.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

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

TKIP regularly changes and rotates 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 pair-wise key 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.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

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), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

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.

34.1.2 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 (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

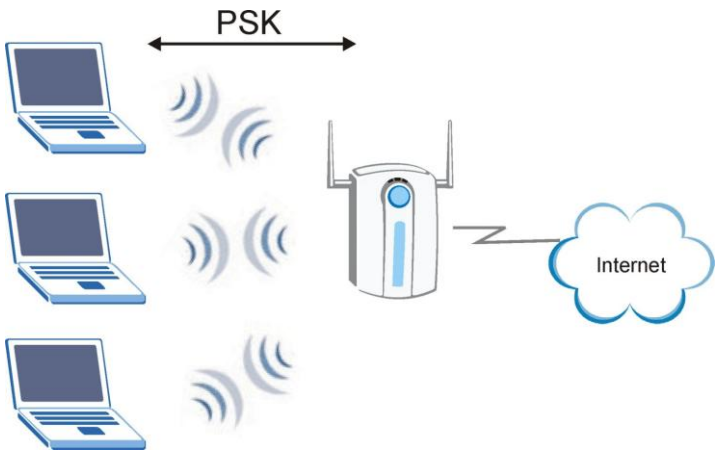


Figure 174 WPA(2)-PSK Authentication

34.1.3 WPA(2) with RADIUS Application Example

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 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 pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Wireless Security Relational Matrix			
AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	**ENCRYPTION 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	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

Appendix E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **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**. Please refer to RFC 1700 for further information about port numbers.
  - 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.

Commonly Used Services			
NAME	**PROTOCOL**	**PORT(S)**	**DESCRIPTION**
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.

AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
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	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example 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 Program, 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 or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management 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.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
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).
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.
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	Simple File Transfer Protocol.
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.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
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.
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.

TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Appendix F

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.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- 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 device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1. this device may not cause interference and
2. this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

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 your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

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.

End-User License Agreement for "VFG6005/VFG6005N"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN–IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS") UNDER GNU GENERAL PUBLIC LICENSE(GPL) or GPL LIKE LICENS. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND

YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no

express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8. Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS,

ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9. Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10. Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11. General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. Please refer to this URL to get more GPL information: http://us.zyxel.com/opensource. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.