Corinex
ADSL2+ Wireless Gateway G

Corinex

User Guide

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of the license. The content of this document is furnished for informational use only, it is subject to change without notice, and it does not represent a commitment on the part of Corinex Communications Corp.

Corinex Communications Corp. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

It is our policy to enhance our products as new technologies, hardware components, software and firmware become available; therefore, the information contained in this document is subject to change without notice.

Some features, functions, and operations described in this document may not be included and sold in certain countries due to government regulations or marketing policies.

The use of the product or its features described in this document may be restricted or regulated by law in some countries. If you are unsure which restrictions or regulations apply, you should consult your regional Corinex office or the authorized reseller.

Published by:
Corinex Communications Corp.
#670-789 West Pender Street
Vancouver, B.C.
Canada V6C 1H2
Tel.: +1 604 692 0520
Fax: +1 604 694 0061

NOTE: This equipment has been tested and found to comply with the limits for Class B information technology equipment. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment 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 equipment does cause harmful interference, the end user is advised to take adequate measures.

2005-04-21 ver. 1

CORINEX COMMUNICATIONS CORPORATION

This End User License Agreement ("EULA") is a legal agreement between you and CORINEX COMMUNICATIONS CORPORATION ("CORINEX") with regard to the copyrighted Software provided with this EULA.

Use of any software and related documentation ("Software") provided with a CORINEX hardware product, or made available to you by CORINEX via download or otherwise, in whatever form or media, will constitute your acceptance of these terms, unless separate terms are provided by the software supplier, in which case certain additional or different terms may apply. If you do not agree with the terms of this EULA, do not download, install, copy or use the Software.

1. Licence Grant. CORINEX grants to you a personal, non-transferable and non-exclusive right to use the copy of the Software provided with this EULA. You agree you will not copy the Software except as necessary to use it on a single hardware product system. You agree that you may not copy the written materials accompanying the Software. Modifying, translating, renting, copying, transferring or assigning all or part of the Software, or any rights granted hereunder, to any other persons, and removing any proprietary notices, labels or marks from the Software is strictly prohibited. Furthermore, you hereby agree not to create derivative works based on the Software. You may permanently transfer all of your rights under this EULA, provided you retain no copies, you transfer all of the Software, and the recipient agrees to the terms of this EULA. If the Software is an upgrade, any transfer must include all prior versions of the Software.

2. Copyright. The Software is licensed, not sold. You acknowledge that no title to the intellectual property in the Software is transferred to you. You further acknowledge that title and full ownership rights to the Software will remain the exclusive property of Corinex Communications Corporation and/or its suppliers, and you will not acquire any rights to the Software, except as expressly set forth above. All copies of the Software will contain the same proprietary notices as contained in or on the Software.

3. Reverse Engineering. You agree that you will not attempt, and if you are a corporation, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, modify, translate or disassemble the Software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder to CORINEX.

4. Disclaimer of Warranty. The Software is provided "AS IS" without warranty of any kind. CORINEX and its suppliers disclaim and make no express or implied warranties and specifically disclaim warranties of merchantability, fitness for a particular purpose and non-infringement of third-party rights. The entire risk as to the quality and performance of the Software is with you. Neither CORINEX nor its suppliers warrant that the functions contained in the Software will meet your requirements or that the operation of the Software will be uninterrupted or error-free.

5. Limitation of Liability. Corinex's entire liability and your exclusive remedy under this EULA shall not exceed the price paid for the Software, if any. In no event shall CORINEX or its suppliers be liable to you for any consequential, special, incidental or indirect damages of any kind arising out of the use or inability to use the software, even if CORINEX or its supplier has been advised of the possibility of such damages, or any claim by a third party.

6. Applicable Laws. This EULA will be governed by the laws of Canada, excluding its conflict of law provisions.

7. Export Laws. This EULA involves products and/or technical data that may be controlled under any applicable export control laws, and regulation, and may be subject to any approval required under such laws and regulations.

8. Precedence. Except as set out above, where separate terms are provided by the software supplier, then, subject to this EULA, those terms also apply and prevail, to the extent of any inconsistency with this EULA.

Contents

1 Introduction

1.1 Overview

Congratulations on your choice of the *Corinex ADSL2+ Wireless Gateway G*! This Gateway is the ultimate residential high speed Internet connectivity solution featuring a built-in ADSL2+ modem and access through Ethernet and wireless (802.11g Wireless) media. Multiple users can share one broadband connection for high speed applications such as shared Internet access, file and printer sharing, on-line games, Internet telephony, streaming audio and video, security systems and more. The *Corinex ADSL2+ Wireless Gateway G* also makes your home network secure with its built-in firewall and enhanced security features.

1.2 Corinex ADSL2+ Wireless Gateway G Features

The *Corinex ADSL2+ Wireless Gateway G* contains an HTTP server with a web configuration interface. This enables you to connect to it, and configure it, using your web browser.

For game users, the ADSL Router had already pre configured for several low latency game ports. Just click on the game you are playing on line and the rest is done for you.

The ADSL Router is fully compatible with all PCs; as long as the PC supports an Ethernet interface and is running a TCP/IP protocol stack, your PC can have high-speed WAN access. So, plug in the ADSL Router (refer to easy start guide), configure it (per your ISP's requirements) and enjoy the fast Internet access like never before. This router also provides future proof functionality with higher data transmission rates with ADSL2, ADSL2+, Extended Reach-ADSL support.

1.2.1 Main Functions

ADSL/ATM Support

- ANSI T1.413 issue 2, ITU-T G.992.1 (G.dmt) and G.992.2 (G.lite) compliant
- ADSL2, ADSL2+, RE-ADSL compliant
- Rate Adaptive modem at 32 Kbps steps
- Dynamic Adaptive Equalisation to improve Carrier's service area
- Bridge Tap Mitigation support
- ATM Layer with Traffic shaping QoS Support (UBR, CBR, VBR-rt, VBR-nrt)
- AAL ATM Attributes - AAL5

- Multiple PVC up to 8 support (Bridge Support)
- Spectral compatibility with POTS
- F5 OAM Loopback/Send and Receive

Encapsulation Support

- RFC2684 Bridge and Routed LLC and VC Mux support
- RFC2364 PPPoA Client support
- RFC2516 PPPoE Client support
- RFC2225/RFC1577 Classical IP Support
- Transparent Bridge Support
- PAP/CHAP/MS-CHAP for Password Authentication Support

Network Support

- Static IP, Dynamic RIP routing support
- IP/TCP/UDP/ICMP/ARP/RARP Application Support
- Network Address Translation (NAT)
- Port Mapping/Forwarding
- Easy setup of Port Forwarding rules for popular Games/Application
- NAT Application Level Gateway for popular applications
- DHCP Server/Relay/client
- DNS Relay Agent
- DMZ support
- Single Session IP Sec and PPTP/L2TP VPN pass through support
- PPP Always on with configurable timeout
- PPP Dial on Demand
- Universal Plug and Play Support

WLAN Support

- IEEE 802.11, 802.11B and 802.11G compliant
- Conforms to Wireless Ethernet Compatibility Alliance (WECA) Wireless Fidelity (Wi-Fi tm) standard
- Supports 802.11b and 802.11g simultaneously
- Support Direct Sequence Spread Spectrum (DSSS) technology
- Operating Range of >300 Meters (Open Air)

Management Support

- Web Based HTTP management GUI
- TFTP/FTP Support for Firmware Upgrade
- Web Based Firmware Upgrade (Local)
- Soft Factory Reset Button via Web GUI
- Diagnostic Test (DSL, OAM, Network, Ping Test)
- Telnet/CLI (Read Only)

- Syslog Support
- Firmware upgrade-able for future feature enhancement

Security Support

- NAT for basic Firewall support
- Packet Filtering Firewall Support
- Stateful Packet Inspection Support
- Protection against Denial of Service attacks
- Password Authentication to Modem

1.3 Package Content

This Package Includes:

- *Corinex ADSL2+ Wireless Gateway G*
- AC power adapter with the appropriate plug for your region
- Telephone cable
- Ethernet cable
- USB cable
- Printed Quick Start Guide
- CD with documentation and drivers

Enclosed CD Content:
- *Corinex ADSL2+ Wireless Gateway G* Quick Start Guide
- *Corinex ADSL2+ Wireless Gateway G* User Guide (this document)
- USB Drivers for Windows operating systems
- Acrobat Reader

As we do constant improvement of our products, it can happen that we have newer versions of software tools than those included on the Installation CD. If you want to check and/or download the latest versions of software for your Corinex product, just click the www.corinex.com.

1.4 Minimum System Requirements

- Pentium® MMX 233MHz
- Ethernet card installed with TCP/IP Protocol (Required only if you are connecting to the Ethernet port of your Gateway)
- One USB 1.1 port (Required if you are connecting to the USB port of the gateway)
- IEEE 802.11b/g Wireless adapter (Required if you are connecting to the gateway using a wireless connection)
- Windows/Linux/Mac OS for Ethernet or Wireless connection, Microsoft Windows 98SE/ME/2000/XP for USB connection
- Web Browser support:
    - Microsoft Internet Explorer 4.0 (or later versions)
    - Netscape® Navigator 3.02 (or later versions)
    - Mozilla Firefox 1.0 (or later versions)
- Windows 98/ME/2000/NT/XP, Mac OS X or Linux operating system for computers sharing the Internet connection
- Web browser supporting JavaScript for the Gateway management

2 Product Specification

This section defines the hardware and software specifications.

2.1 Hardware Features

2.1.1 Hardware Parameters

WAN Interface

- WAN: 1x RJ11 connector for connection to the ADSL line

Ethernet Interfaces

- LAN: 4 x 10/100 Mbps Ethernet Port (RJ-45)
- WAN: 1 x RJ-11 port (25 Mbps)
- USB: 1x USB 1.1 Type B

Electrical Parameters

One AC power adapter for power supply

Input Voltage:	AC 110/230V (USA/Europe), 150mA
Line Frequency:	60/50Hz (USA/Europe)

Wireless Parameters

RF Output : <= 100 mW

Environmental Parameters

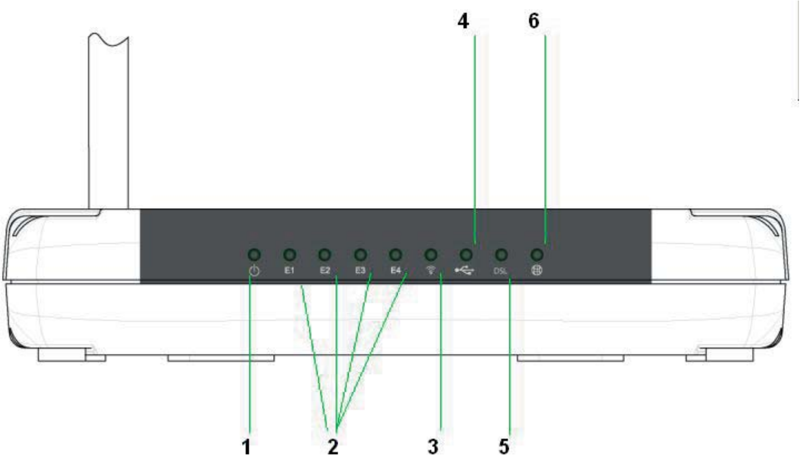
Operation	Operating Temperature: 0°C to 40°C (32°F to 104°F)
	Operating Humidity 10% to 85% Non-Condensing
Storage	Storage Temp: -20°C to 70°C (-4°F to 158°F)
	Storage Humidity 5% to 90% Non-Condensing

EMI/EMC

FCC Part 15B, UL, CE (EMI, EMC, Safety)

2.2 Physical Details

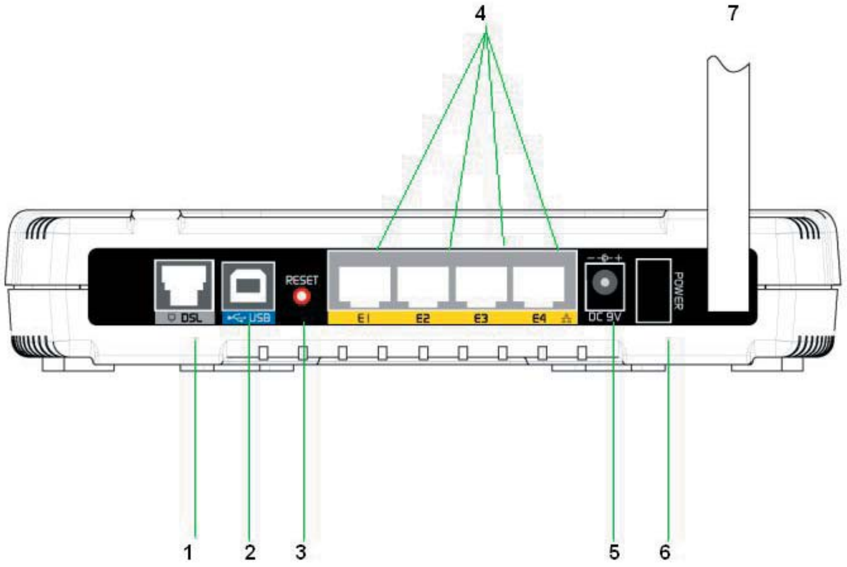
Front Panel



1 POWER	green	On	Power is supplied to the gateway.
		Off	The gateway is turned off.
2 ETHERNET (E1 ~ E4)			
	green	On	Connection established between the gateway and the Ethernet device.

		Off	Ethernet cable is disconnected.
		Blinking	Receiving/transmitting data.
3 WIRELESS	green	Blinking	Receiving/transmitting data via wireless interface.
4 USB	green	On	Connection established between the gateway and the computer's USB slot.
		Off	USB cable not connected.
5 DSL	green	On	ADSL connection is established.
		Off	No telephone jack is connected.
		Blinking	The gateway is attempting to establish a connection with your ADSL Service Provider.
6 INTERNET	green	On	PPP connection is established.
		Off	No PPP connection is established.

Back Panel



1 DSL (RJ-11) to connect to your DSL line.
2 USB to connect to your PC's USB slot.
3 RESET to reset your ADSL2+ Gateway to factory default settings.
4 ETHERNET E1-E4 (10/100 Base-T Auto-MDI/MDIX RJ-45 jack) to connect to your PC's Ethernet Network card or Ethernet Hub / Switch.

5 DC IN (9V) to connect to the Power Supply Adapter.
6 POWER SWITCH to power on or off the gateway (I - ON position, O - OFF position).
7 RF Antenna 180° 2.4 Ghz Wireless Antenna for wireless networking.

To activate the factory default reset function:

- *Ensure that your ADSL2+ Gateway is powered on.*
- *Use a paper clip or a pencil tip to press the reset button, hold for at least 10 secs and release. At this point, the Wireless indicator and DSL indicator will turn off. The reset is in progress.*
- *When the Wireless indicator starts blinking, it means that the reset process is complete. The default settings are then restored.*
- *DSL line is synchronized once the DSL indicator* color is green.

> **NOTE:** By executing the reset procedure, all customized settings that you have saved will be lost and the gateway will be set back to the original factory default settings as they are described in this document.

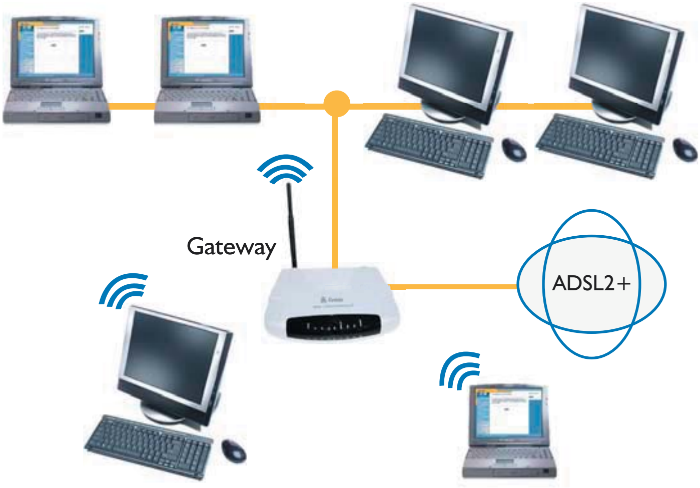
2.3 Safety Labels

Content of the Label on the Bottom of the Corinex ADSL2+ Wireless Gateway G

The label shows the voltage and current values for your Gateway. It also shows all three MAC Addresses (WAN, LAN and WLAN), serial number (SN) and the firmware version.

3 Installation Overview

This part of the User Guide will assist you with your initial installation and configuration of your network and help you with settings, which you need to configure for your Internet connection to be shared through Ethernet, USB or Wireless media.



3.1 Connecting the Gateway to Your Computer

This chapter gives step-by-step instructions on how to connect your computer to the gateway, connect the gateway to your ADSL line, and finally, to turn on all the devices.

3.1.1 Connecting to the Ethernet

Connect your computer(s) to the *ADSL2+ Wireless Gateway G* by plugging one end of the supplied Ethernet cable (RJ45) to the network card of your computer, and the other end of the cable to one of the gateway's four Ethernet LAN ports (E1~E4).

NOTE: If you want to connect more computers to the gateway via Ethernet cables, follow the same procedure as described above. Please note that if you want to connect more than four computers in this way, an additional device (a switch or a hub) is required.

3.1.2 Connecting to the ADSL Line

To connect the gateway to the ADSL line, please use the supplied telephone cable (RJ11). Plug one end of the cable to the DSL port of the gateway, and plug the other end of the telephone cable into the telephone socket in the wall. If you want to plug a phone in at the same location, you will need to use a POTS splitter.

A POTS Splitter (with built-in Microfilter) is a device that allows you to connect both your telephone cable and telephone set to the same wall socket. At the same time, this splitter helps to eliminate background noise on the telephone line, ensuring the best possible phone performance.

3.1.3 Connecting to the Power Outlet and Powering On

1. Connect the supplied power supply cable to the DC 9V port on the gateway.
2. Plug the power adapter into the electrical outlet.
3. Power on the gateway by toggling the POWER switch into position I.
4. Start up all computers in the network.

3.2 Configuring Your Ethernet Network Card / Installing Your USB Device

If your computers are connected to the Ethernet Port of the gateway, proceed with section 3.2.1. If your computer is connected to the gateway's USB Port, you can skip ahead to section 3.2.2.

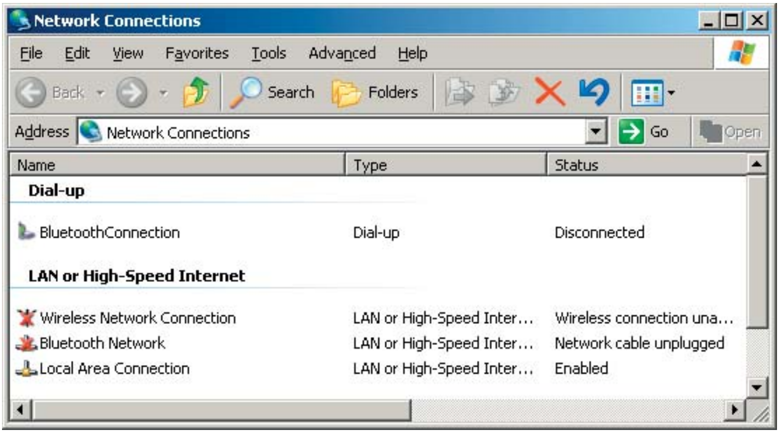
3.2.1 Configuring Your Ethernet Network Card

Proceed with this section ONLY if your computer is connected to the Ethernet Port of the gateway.

The following instructions are based on the Windows XP operating system. The configuration procedure may be slightly different on other operating systems. Please refer to the documentation of your operation system for more information about establishing a network connection.

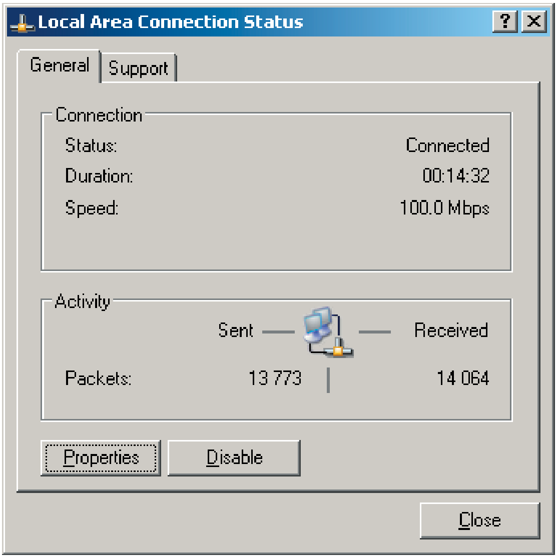
(Instructions are based on default Start menu option)

1. From your Windows desktop, click **Start > All Programs > Accessories > Communications > Network Connections**.


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go Open

Name	Type	Status
Dial-up		
BluetoothConnection	Dial-up	Disconnected
LAN or High-Speed Internet		
Wireless Network Connection	LAN or High-Speed Inter…	Wireless connection una…
Bluetooth Network	LAN or High-Speed Inter…	Network cable unplugged
Local Area Connection	LAN or High-Speed Inter…	Enabled

2. Right-click on the **Local Area Connection** icon that reflects the model of Ethernet Card which you have connected to the *Corinex ADSL2+ Wireless Gateway G*, and click **Properties**.

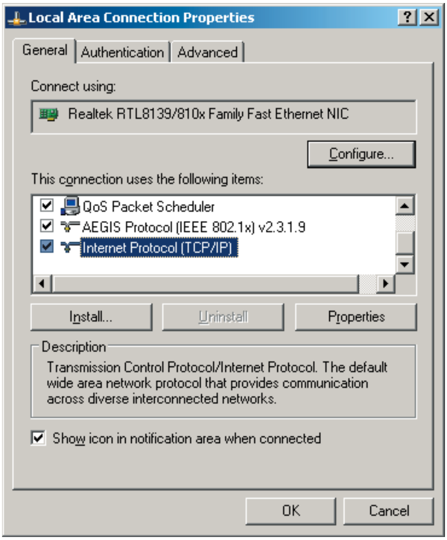


Connection
Status: Connected
Duration: 00:14:32
Speed: 100.0 Mbps

Activity
Sent — — Received
Packets: 13 773 | 14 064

3. Make sure that the field **Connect Using** indicates the model of Ethernet Card that is connected to the gateway. (This is important especially if you have more than one **Local Area Connection** icon displayed in the **Network and Dial-up Connections/Network Connections** window. Make sure that you have selected the appropriate one.)

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



Local Area Connection Properties

Connect using:

Realtek RTL8139/810x Family Fast Ethernet NIC

This connection uses the following items:

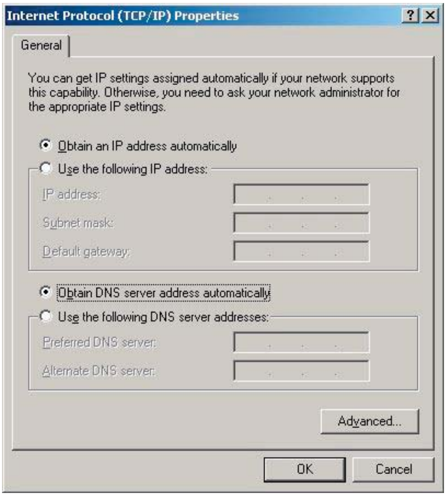
- ☑ QoS Packet Scheduler
- ☑ AEGIS Protocol (IEEE 802.1x) v2.3.1.9
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

5. Select the option **Obtain an IP address automatically** and click **OK**.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

6. Click **OK** again to close.

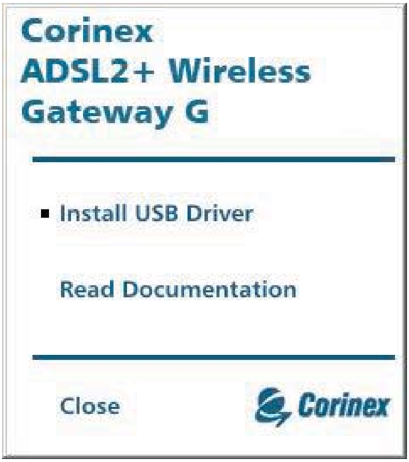
7. Make sure that the *ADSL2+ Wireless Gateway G* is powered on. Restart your system.

8. Follow the above steps 1-7 for all computers connected to the gateway through the Ethernet interface.

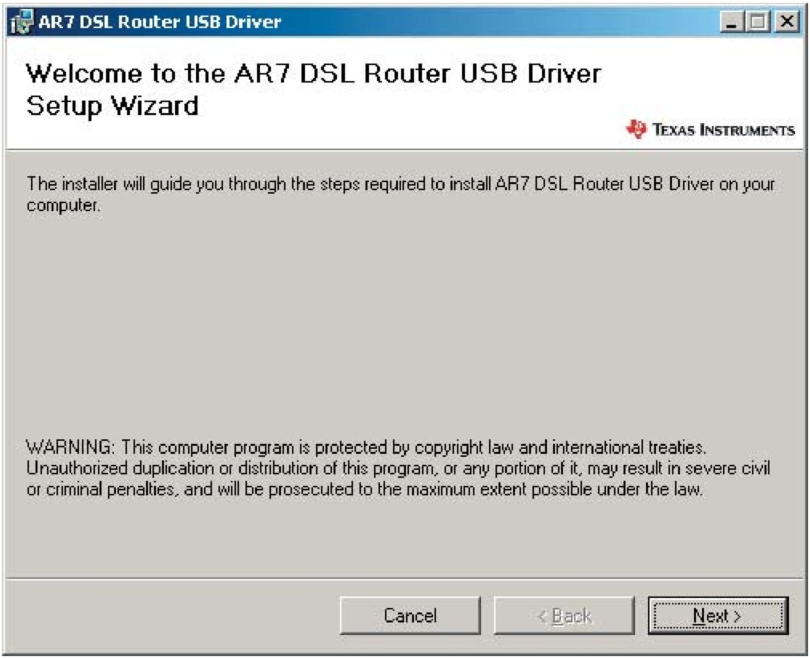
3.2.2 Installing the USB Device Driver

Note: Please do not connect the *Corinex ADSL2+ Wireless Gateway G* to your computer before step #2.

1. Insert the *Corinex ADSL2+ Wireless Gateway G* CD into the CD-ROM drive of your computer. If the installation wizard doesn't start automatically, please navigate to the main folder of the installation CD (with Windows Explorer or any other file browser program) and run the program named **autorun.exe**. Click **Install USB Drivers**. The wizard for the USB driver installation will start. Please wait until the installation of the drivers is finished and then click **Close** to finish the installation wizard.



Click **Install USB Drivers**. The wizard for the USB driver installation will start. Please wait until the installation of the drivers is finished and then click **Close** to finish the installation wizard.



AR7 DSL Router USB Driver

Welcome to the AR7 DSL Router USB Driver Setup Wizard

The installer will guide you through the steps required to install AR7 DSL Router USB Driver on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

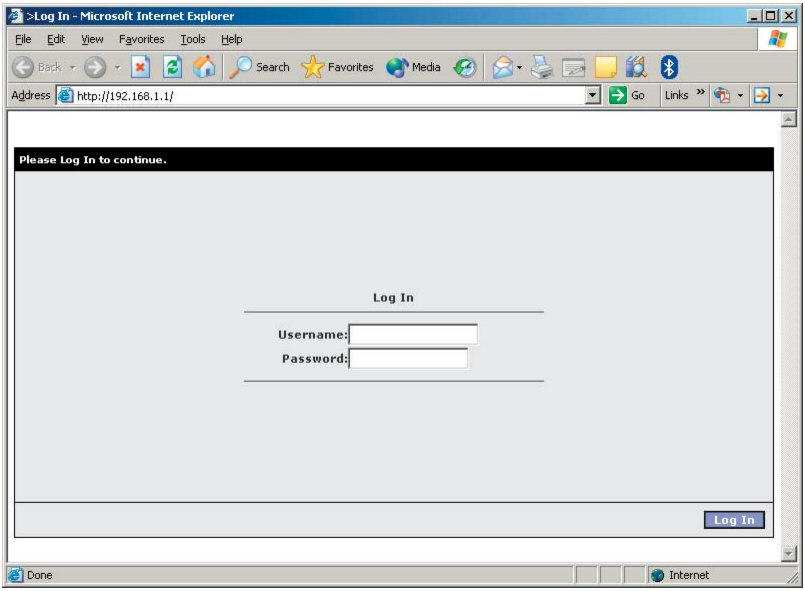
2. Plug the *Corinex ADSL2+ Wireless Gateway G* into a USB port on your computer. These are often located on the front on desktop computers, and on the back on laptops.

3. Windows will detect new hardware and will start installing it. If a box pops up asking whether Windows should connect to Windows Update to search for software, choose **No, not at this time** and click **Next**. This screen will only occur if you have Windows XP Service Pack 2 installed. Then choose **Install the software automatically** and click **Next**. You may get a security warning about the drivers not being Microsoft-certified or not passing Microsoft Logo testing, but click **Continue Anyway**. The installation of the USB driver is now complete. You may click **Finish**.

3.3 Connecting to the Internet

If you want to configure the *Corinex ADSL2+ Wireless Gateway G*'s connection to the internet, you can access the device through the web user interface by following these steps:

1. Open your Internet Browser and enter 192.168.1.1 in the address bar, and press **Enter**.



>Log In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Done
Internet
Log In

Address http://192.168.1.1/

Please Log In to continue.

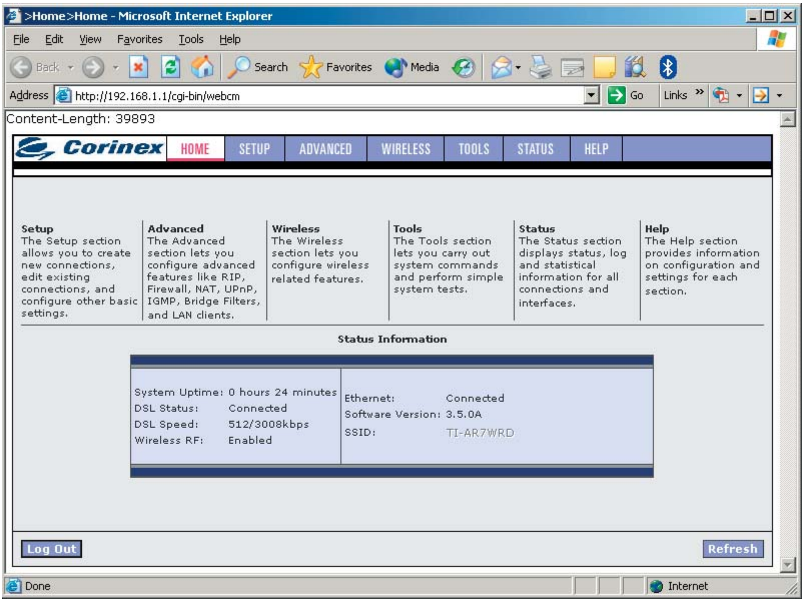
Log In

Username:

Password:

You will be asked for the username and password. The default username is **admin** and the password is **admin**.

2. Upon Login, the main page will be displayed.


>Home>Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/cgi-bin/webcm
Go Links
Corinex
HOME SETUP ADVANCED WIRELESS TOOLS STATUS HELP
Log Out
Refresh
Done
Internet

Content-Length: 39893

Setup The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

Advanced The Advanced section lets you configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, and LAN clients.

Wireless The Wireless section lets you configure wireless related features.

Tools The Tools section lets you carry out system commands and perform simple system tests.

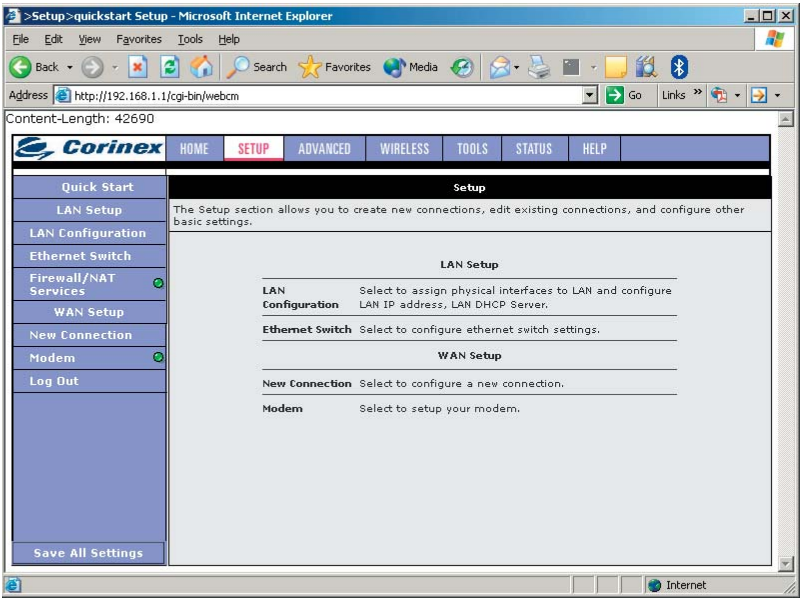
Status The Status section displays status, log and statistical information for all connections and interfaces.

Help The Help section provides information on configuration and settings for each section.

Status Information

System Uptime:	0 hours 24 minutes	Ethernet:	Connected
DSL Status:	Connected	Software Version:	3.5.0A
DSL Speed:	512/3008kbps	SSID:	TI-AR7WRD
Wireless RF:	Enabled		

Click on **Setup** in the upper bar. The following window will appear.


>Setup>quickstart Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/cgi-bin/webcm
Go Links
Corinex
HOME SETUP ADVANCED WIRELESS TOOLS STATUS HELP
Quick Start
LAN Setup
LAN Configuration
Ethernet Switch
Firewall/NAT Services
WAN Setup
New Connection
Modem
Log Out
Save All Settings
Internet

Content-Length: 42690

Setup

The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

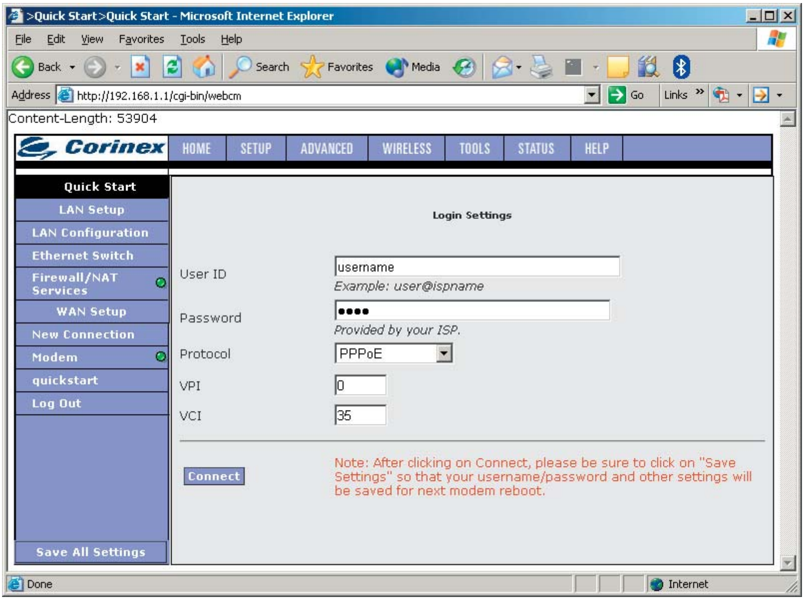
LAN Setup

LAN Configuration	Select to assign physical interfaces to LAN and configure LAN IP address, LAN DHCP Server.
Ethernet Switch	Select to configure ethernet switch settings.

WAN Setup

New Connection	Select to configure a new connection.
Modem	Select to setup your modem.

3. In the left menu bar, click on **Quick Start** to start the internet connection wizard. The following screen will appear.



Content-Length: 53904

Login Settings

User ID: username
Example: user@ispname

Password: ●●●●
Provided by your ISP.

Protocol: PPPoE

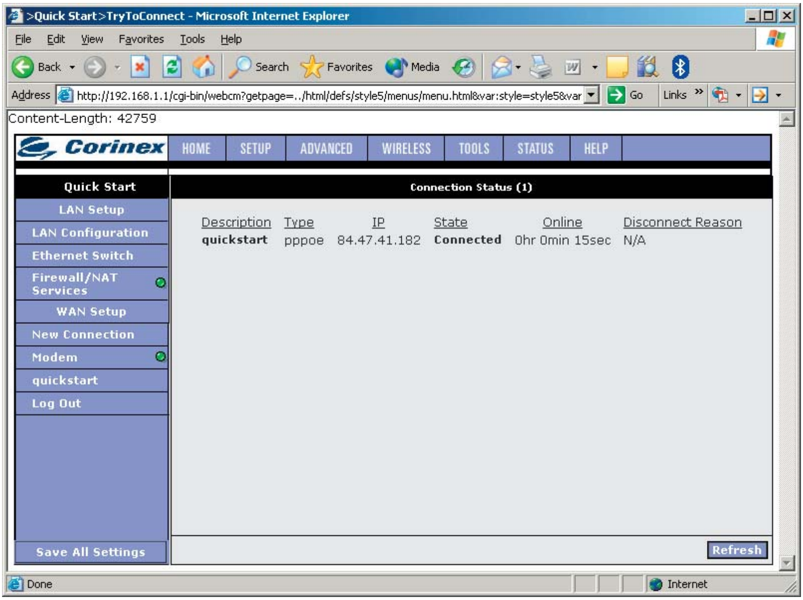
VPI: 0

VCI: 35

Note: After clicking on Connect, please be sure to click on "Save Settings" so that your username/password and other settings will be saved for next modem reboot.

4. All the information you need for this screen should have already been provided to you by your Internet Service Provider. Please carefully fill in all required fields and click on **Connect**.

5. The gateway will now connect to your Internet Service Provider. A few screens displaying the connection status will appear. If all the required authentication data was entered correctly and the gateway is connected to the DSL line, a screen similar to the one below will appear.



>Quick Start>TryToConnect - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/cgi-bin/webcm?getpage=../html/defs/style5/menus/menu.html&var:style=style5&var
Go Links
Corinex
HOME SETUP ADVANCED WIRELESS TOOLS STATUS HELP
Quick Start
LAN Setup
LAN Configuration
Ethernet Switch
Firewall/NAT Services
WAN Setup
New Connection
Modem
quickstart
Log Out
Save All Settings
Refresh
Done
Internet

Content-Length: 42759

Connection Status (1)

Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	84.47.41.182	Connected	0hr 0min 15sec	N/A

6. Your *ADSL2+ Wireless Gateway G* is now connected to the internet.

7. Click on **Save All Settings** once you've successfully established a connection, so that all settings are saved. Your gateway will then connect to the internet automatically after restart.

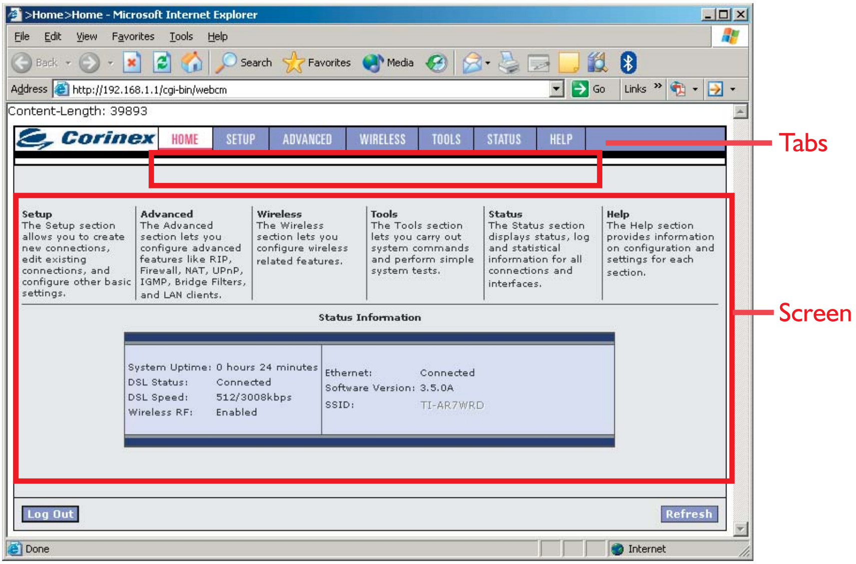
4 Corinex ADSL2+ Wireless Gateway G Configuration

4.1 Overview

For your convenience, use the *Corinex ADSL2+ Wireless Gateway G* web-based utility to configure it. This chapter will explain all of the functions of this utility. The utility can be accessed via Microsoft Internet Explorer, Netscape Navigator, Mozilla Firefox or other web browsers to set up Ethernet, Wireless, or USB computer connections to the *Corinex ADSL2+ Wireless Gateway G*. This utility has a consistent design for all of its screens. It consists of screen selection tabs on the top part of screen, menu on the left side and the display screen.

> **NOTE:** The appearance of the user interface screenshots displayed in the following part of this document may vary due to the firmware version currently available in your device. It is recommended that you check for the latest firmware version on the Corinex web site: www.corinex.com.

After opening the default gateway's IP address 192.168.1.1 in your internet browser, the authentication screen appears. Please enter the username **admin** and the password **admin** in order to get to the main screen.


>Home>Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/cgi-bin/webcm
Go Links
Corinex
HOME
SETUP
ADVANCED
WIRELESS
TOOLS
STATUS
HELP
Tabs
Screen
Log Out
Refresh
Done
Internet

Content-Length: 39893

Setup
The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

Advanced
The Advanced section lets you configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, and LAN clients.

Wireless
The Wireless section lets you configure wireless related features.

Tools
The Tools section lets you carry out system commands and perform simple system tests.

Status
The Status section displays status, log and statistical information for all connections and interfaces.

Help
The Help section provides information on configuration and settings for each section.

Status Information

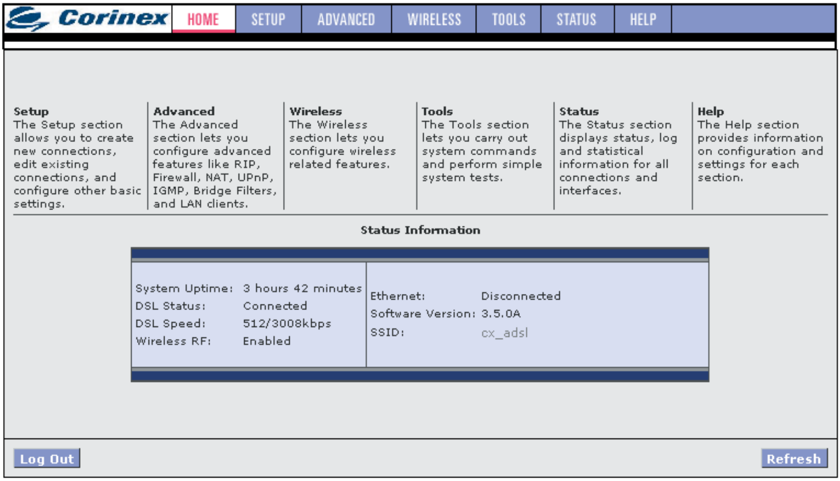
```
System Uptime: 0 hours 24 minutes     Ethernet:          Connected
DSL Status:    Connected              Software Version:  3.5.0A
DSL Speed:     512/3008kbps           SSID:              TI-AR7WRD
Wireless RF:   Enabled
```

As you click on the selection tabs, different screens will be displayed.

The **Home**, **Setup**, **Advanced**, **Wireless**, **Tools**, **Status** and **Help** tabs are available for setup of the *Corinex ADSL2+ Wireless Gateway G*. In each of these tabs groups there is a Menu on left side. From here you can access and change different settings of your gateway. The display screen consists of one or more entry fields containing current values of the settings. By changing these values you can configure the device. To apply the settings of your choice you have to click on the **Save All Settings** button located on the left bottom of the web interface under the left menu. The settings will be entered into the gateway.

4.2 Main tab

After logging in to the Gateway's configuration web interface, the following page will appear:



Setup
The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

Advanced
The Advanced section lets you configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, and LAN clients.

Wireless
The Wireless section lets you configure wireless related features.

Tools
The Tools section lets you carry out system commands and perform simple system tests.

Status
The Status section displays status, log and statistical information for all connections and interfaces.

Help
The Help section provides information on configuration and settings for each section.

Status Information

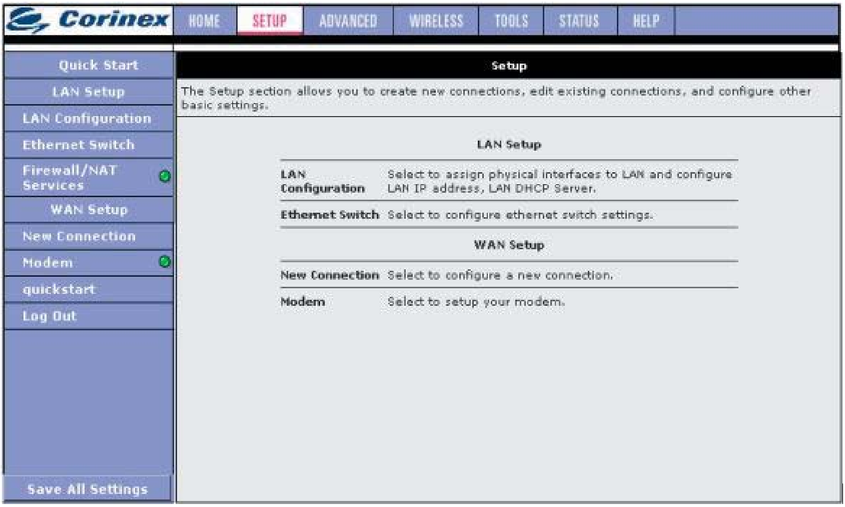
System Uptime:	3 hours 42 minutes	Ethernet:	Disconnected
DSL Status:	Connected	Software Version:	3.5.0A
DSL Speed:	512/3008kbps	SSID:	cx_adsl
Wireless RF:	Enabled		

Here you can see the basic information about each tab, together with basic information about the status of the *ADSL2+ Wireless Gateway G*. For example, the screen above shows that the gateway has been connected to the DSL line for more than 3 hours with upload speed 512 kbps and download speed of 3008 kbps. Wireless access point is enabled with the SSID cx_adsl and there are no devices connected to the 4-port ethernet switch. Additionally, you can see the firmware version.

4.3 Setup tab

The Setup section allows you to create new connections, edit existing connections, and configure other basic settings. This section is divided into three parts: the first one is “Quick Start” which helps you with creating a WAN connection. The second one is “LAN Setup” where you can configure the local area network settings. In the third part “WAN Setup”, you can set up the modem and the WAN parameters.

The following picture shows the setup page.



Setup

The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

LAN Setup

LAN Configuration	Select to assign physical interfaces to LAN and configure LAN IP address, LAN DHCP Server.
Ethernet Switch	Select to configure ethernet switch settings.

WAN Setup

New Connection	Select to configure a new connection.
Modem	Select to setup your modem.

The page is divided into three subsections – the **Quick Start**, the **LAN** and the **WAN** configuration.

Before configuring the Gateway, there are several concepts that you should be familiar with on how your new Gateway works. Please take a moment to familiarize yourself with these concepts, as it should make the configuration much easier.

Wide Area Network connection

On one side of the Gateway there is your Wide Area Network (WAN) connection, also referred to as a broadband connection. This WAN connection is different for every WAN operator. Most of the configuration you will perform will be in this area.

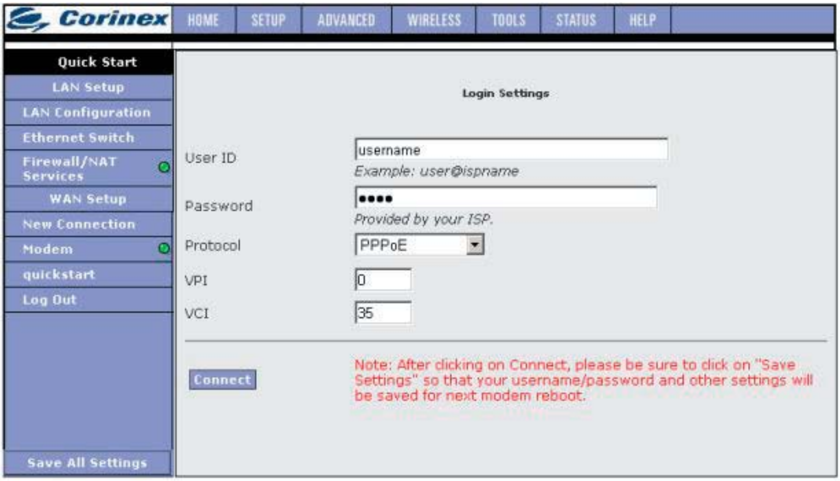
Local Area Network connection

On the other side of your Gateway, you have your own Local Area network (LAN) connections. This is where your local computers are connected to the Gateway. The Gateway is normally configured to automatically assign IP addresses for all the PC's on your network.

4.3.1 Quick Start

For your convenience, we have prepared a setup wizard which will allow you to connect your Gateway to the internet in a few easy steps.

Click on **Quick Start** located on top of the left menu. The following screen will appear.



Login Settings

User ID: username
Example: user@ispname

Password: ••••
Provided by your ISP.

Protocol: PPPoE

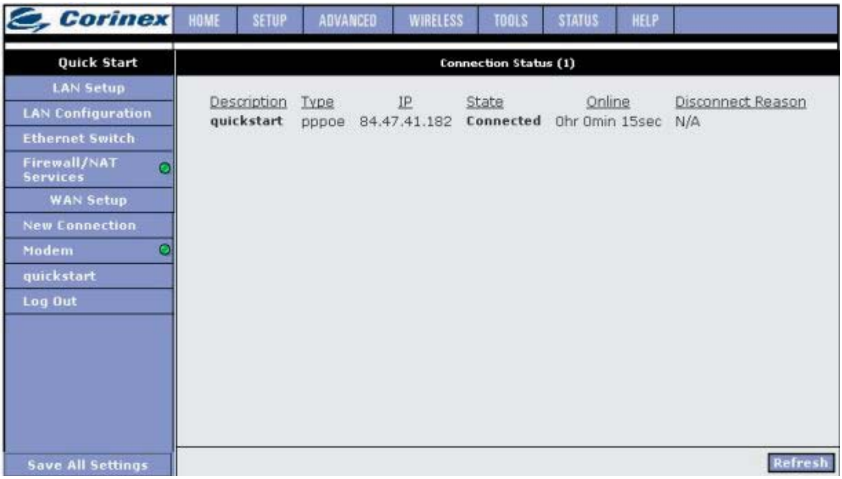
VPI: 0

VCI: 35

Note: After clicking on Connect, please be sure to click on "Save Settings" so that your username/password and other settings will be saved for next modem reboot.

All information for creating a connection should be provided by your Internet Service Provider. Please enter the necessary information into the fields on this screen. If you are not sure, please contact your Internet Service Provider. Click **Connect**.

The gateway will now connect to your Internet Service Provider. A few screens displaying the connection status will appear. If all the required authentication data was entered correctly and the gateway is connected to the DSL line, a screen similar to the one below will appear.



Connection Status (1)

Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	84.47.41.182	Connected	0hr 0min 15sec	N/A

Note: if you receive an error message, please double check that the Gateway is connected to the DSL line and the entered authentication data are correct.

Your *ADSL2+ Wireless Gateway G* is now connected to the internet.

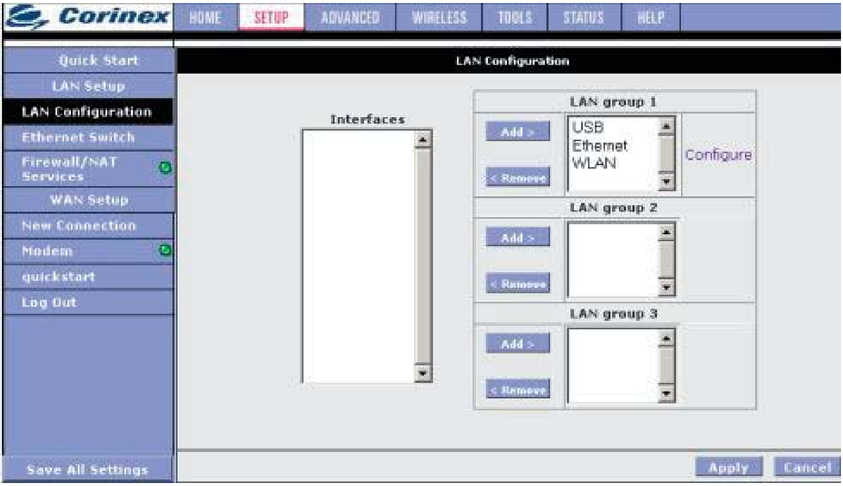
Click on **Save All Settings** once you've successfully established a connection, so that all settings are saved. Your gateway will then connect to the internet automatically after each restart.

4.3.2 LAN Configuration

This section allows you to configure the local area network settings of your Gateway. There are three LAN network interfaces which can be assigned to groups. Each group can have different settings such as IP address, settings of the DHCP server etc.

Physical Network Interface	Description
Ethernet	LAN containing all devices connected to one of the RJ45 ports of the Gateway.
WLAN	LAN containing all devices connected to the wireless access point of the Gateway.
USB	LAN containing all devices connected to the USB port of the Gateway.

By default, all three interfaces belong to the same group – Group 1.



LAN Configuration

Interfaces

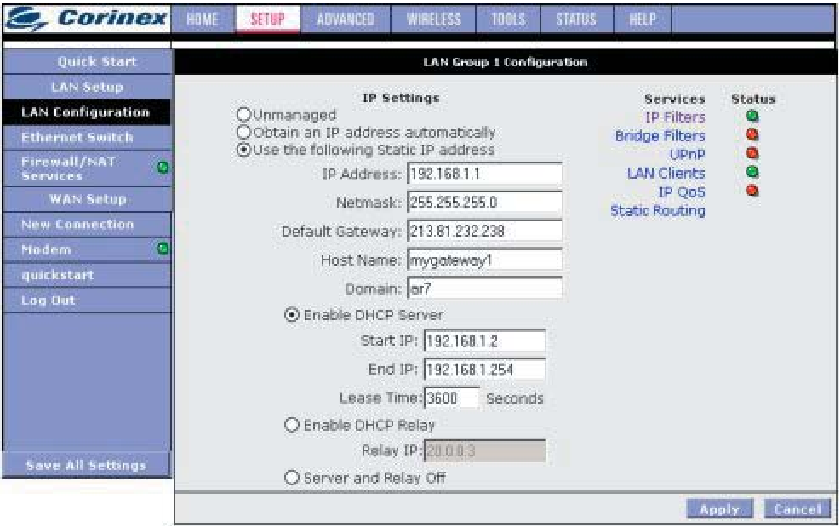
LAN group 1: USB, Ethernet, WLAN

LAN group 2

LAN group 3

In the table **Interfaces** there are interfaces which are not assigned to any group. You can move interfaces between groups using the **Add** and **Remove** buttons next to each group.

You can click on **Configure** to set up parameters for the appropriate LAN Group. You will enter the following screen.



LAN Group 1 Configuration

IP Settings

○ Unmanaged
○ Obtain an IP address automatically
● Use the following Static IP address

IP Address: 192.168.1.1
Netmask: 255.255.255.0
Default Gateway: 213.81.232.238
Host Name: mygateway1
Domain: ar7

● Enable DHCP Server
Start IP: 192.168.1.2
End IP: 192.168.1.254
Lease Time: 3600 Seconds

○ Enable DHCP Relay
Relay IP: 20.0.0.3

○ Server and Relay Off

Services	Status
IP Filters	🟩
Bridge Filters	🟥
UPnP	🟥
LAN Clients	🟩
IP QoS	🟥
Static Routing	

You can choose from **Unmanaged**, **Automatic** or **Static IP** settings for this LAN Group. Unmanaged settings don't require any additional configuration. With the setting "Obtain an IP Address automatically", the LAN group will request the IP Settings from a DHCP server in the LAN.

If you choose the Static IP Settings, you can configure the following fields: **IP Address**, **Netmask**, **Default Gateway**, **Host Name** and **Domain**.

The gateway includes a DHCP server and DHCP relay functionality. You can choose from **Enable DHCP Server**, **Enable DHCP Relay** or **DHCP Server and Relay off**.

You can enable the DHCP Server by clicking the radio button **Enable DHCP Server**.
You will need to specify the **Start IP** Address and **End IP** Address for assigning addresses to clients. With **Lease Time**, you can specify how many seconds a client will hold the assigned IP before it asks for a new one. The default settings is one hour (3600 seconds).

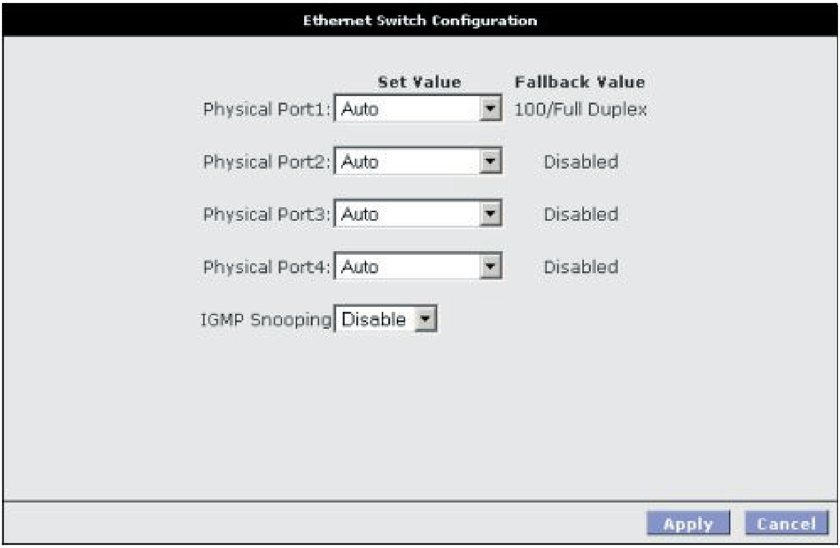
In addition to the DHCP server feature, the Gateway supports the DHCP relay function. When the gateway is configured as a DHCP server, it assigns the IP addresses to the LAN clients. When the Gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server.

By turning off the DHCP server and relay the network administrator must carefully configure the IP address, Subnet Mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer and your ADSL+ Gateway must be on the same subnet as all the other computers.

You can configure additional settings for each LAN Group, by clicking on one of the buttons **IP Filters**, **Bridge Filters**, **UPnP**, **LAN Clients**, **IP QoS** and **Static Routing** on the right side of the LAN Group Configuration screen. This features will be described later in this user guide.

4.3.3 Ethernet Switch

In the next section of the Setup tab, you can configure the 4-port ethernet switch of your Gateway.



Ethernet Switch Configuration

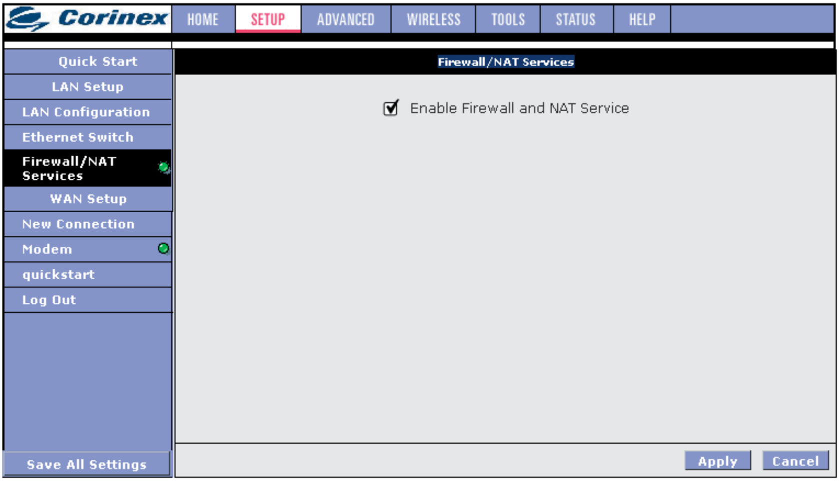
	Set Value	Fallback Value
Physical Port1:	Auto	100/Full Duplex
Physical Port2:	Auto	Disabled
Physical Port3:	Auto	Disabled
Physical Port4:	Auto	Disabled
IGMP Snooping	Disable	

For each of the 4 ports you can select between **Auto**, **10/Half Duplex**, **10/Full Duplex**, **100/Half Duplex** and **100/Full Duplex**. We recommend the Auto setting which makes sure that your ethernet device connected to the switch will work properly.

Additionally, you can enable or disable **IGMP Snooping** for the ethernet switch. IGMP Snooping is a feature whch allows the switch to enable or disable multicast traffic automatically for each port and prevents unwanted traffic going to computers on the network. With IGMP Snooping, Layer 2 devices can “listen in” on IGMP conversations between hosts and routers. When a switch hears a group join message from a host, it notes which switch interface it heard the message on, and adds that interface to the group. Similarly, when a Layer 2 switch hears a group leave message or a response timer expires, the switch will remove that host’s switch interface from the group.

4.3.4 Firewall / NAT Services

For the LAN interfaces, Firewall and NAT are enabled by default. If you don't want to use Firewall or Network Address Translation, you can disable it in the screen below.



Firewall/NAT Services

☑ Enable Firewall and NAT Service

4.3.5 WAN Setup

Before the gateway will pass any data between the LAN interface(s) and the WAN interface, the WAN side of the modem must be configured. Depending upon your DSL service provider or your ISP (internet service provider), you will need some (or all) of the information outlined below before you can properly configure the WAN:

- Your DSL line VPI and VCI
- Your DSL encapsulation type and multiplexing
- Your DSL training mode (default is MMODE)

For PPPoA or PPPoE users, you also need these values from your ISP:
- Your username and password

For RFC 1483 users, you may need these values from your ISP:
- Your DSL fixed Internet IP address
- Your Subnet Mask
- Your Default Gateway
- Your primary DNS IP address

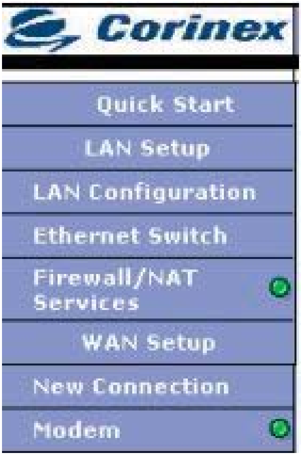
Since multiple users can use the gateway, the gateway can simultaneously support multiple connection types; hence, you must set up different profiles for each connection. The gateway supports the following protocols:

- RFC2516 PPPoE
- RFC 2364 PPPoA
- Static
- DHCP
- Bridged
- CLIP

4.3.6 New Connection

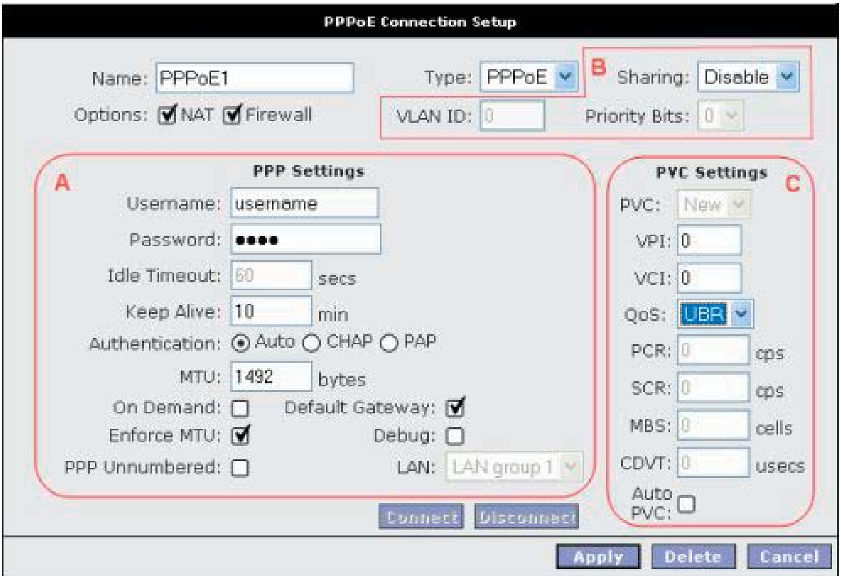
A new connection is basically a virtual connection. Your gateway can support up to 8 different (unique) virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the modem to pass data correctly.

Before you create a new WAN connection, you should make sure you have DSL connection. If you have an existing DSL connection a green light will be displayed in the left menu next to the Modem item as shown in the picture below.



Click on **New Connection** to enter the page for creating and configuring a new connection to the internet. The following page will appear, with predefined settings for a PPPoE connection.

> **Note**: This screen can be virtually divided into three sections. Section **A** includes settings specific to the connection type. Section **B** (VLAN settings) and section **C** (PVC settings) remain the same for all six connection types. For other connection types, we will focus on the fields and features in section **A**.



PPPoE Connection Setup

Name: PPPoE1
Type: PPPoE
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

PPP Settings

Username: username
Password: ●●●●
Idle Timeout: 60 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □
Default Gateway: ☑
Enforce MTU: ☑
Debug: □
PPP Unnumbered: □
LAN: LAN group 1

PVC Settings

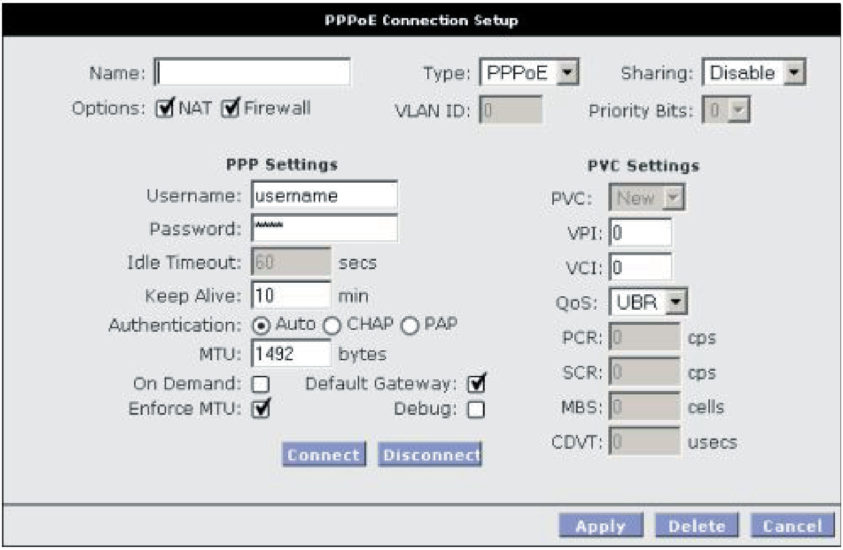
PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

PPPoE Connection Setup

PPPoE is a protocol for encapsulating PPP frames in Ethernet frames and is described in RFC 2516. PPPoE provides the ability to connect to a network of hosts over a simple bridging access device to a remote Access Concentrator. With this model, each host utilizes its own PPP stack and access control, billing, and type of service control can all be done on a per-user rather than per-site basis.

Follow the instructions below to configure the gateway as PPPoE.

1. From the Setup main page, click on **New Connection**.
   The default PPPoE connection setup is displayed. The following picture illustrates a typical PPPoE configuration.



PPPoE Connection Setup

Name:
Type: PPPoE
Sharing: Disable

Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

PPP Settings

Username: username
Password: *****
Idle Timeout: 60 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □
Default Gateway: ☑
Enforce MTU: ☑
Debug: □

PVC Settings

PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs

2. Enter a unique name for the PPPoA connection in the **Name** field. The name must not have spaces and cannot begin with numbers.

3. Under **PPP Settings**, select the encapsulation type (LLC or VC). Note: If you are not sure just use the default mode.

4. Under **PVC Settings**, enter the values of VPI and VCI settings.

Note: Your DSL service provider or your ISP will supply these.

5. Select the quality of service (QOS). Leave the default value if you are unsure or the ISP did not provide this information.

6. Click the **Apply** button to complete the connection setup. This will temporarily save this connection.

7. To make the change permanent, click on **Save all settings** in the left menu.

8. For connection, click on **Connect**.

The available PPPoE options are described in the following table:

Field	Description
Username	Your user name for the PPPoE access; this is provided by your DSL service provider or your ISP.
Password	The password for the PPPoE access; it is provided by your DSL service provider or your ISP.
Idle Timeout	Specifies that PPPoE connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a **0** in this field.
Keep Alive	When on-demand option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field.
Authentication	Three authentication options are available: **auto, Challenge Handshake Authentication protocol** (CHAP), and **Password Authentication Protocol** (PAP).
MTU	Maximum Transmit Unit that the DSL connection can transmit. It is a negotiated value that asks the provider to send packets of no more than n bytes. The maximum specified value is 1500 although some DSL/ISP providers require a larger value. The minimum MTU value is 128.
On-Demand	Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
Default Gateway	If checked, this connection becomes the default gateway to the Internet.
Enforced MTU	Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MRU by changing TCP Maximum Segment Size to PPP MRU.
Debug	Enables PPPoE connection debugging facilities. You can read more about debugging in following text.
PPP UNnumbered	This is a special feature for telecommunication. It is used for assigning blocks of public addresses to the client and makes the PPP appear as pass-through.
LAN	The LAN field associated with the PPP UNunmbered field. The packets need to go through specific LAN when the PPP UNnumbered feature is activated.

The VLAN Settings include the options showed in following table:

Field	Description
Sharing	This is where you enable/disable sharing. The VLAN needs to be selected to create VLAN.
VLAN ID	VLAN Identification
Priority Bits	Priority is given to a VLAN connection from 0-7, 0 means highest priority.

The following table describes the options of the PVC Settings:

Field	Description
PVC	Permanent virtual circuit. A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.
VPI	Virtual path identifier
VCI	Virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. It is sometimes called virtual channel connection.
QoS	Quality of Service, a feature of data transmission that measures how accurately and how quickly a message or data is transferred from a source computer to a destination computer over a network. The three QoS options are: **Undefined Bit Rate** (UBR), **Constant Bit Rate** (CBR), and **Variable Bit Rate** (VBR).
PCR	Peak Cell Rate (in cells/sec) is the cell rate, which the source may never exceed.
SCR	Sustain Cell Rate
MBS	Maximum Burst Size - traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell rate.
CDVT	Cell Delay Variation Tolerance
Auto PVC	Auto Permanent Virtual Circuit, see PVC.

PPPoA Connection Setup

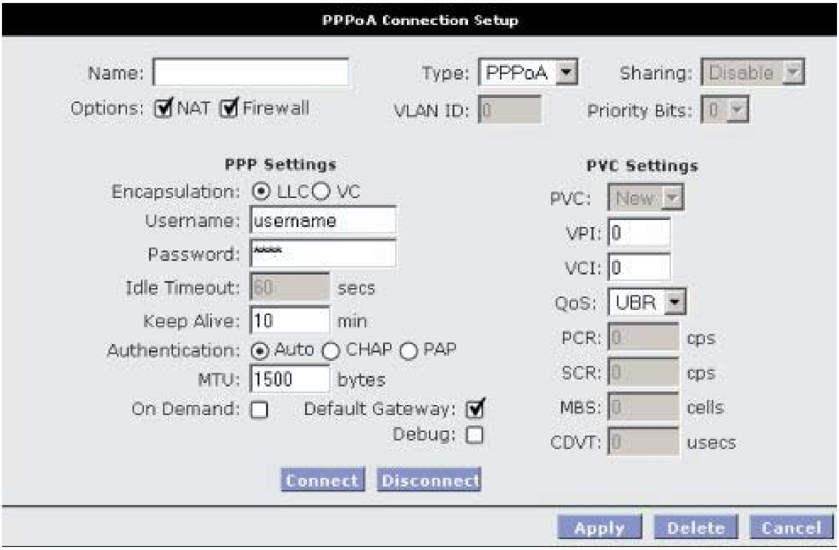
PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets over ATM cells, which are carried over the DSL line. PPP or Point-to-Point protocol is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users. LLC and VC are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

By selecting PPPoA, you are forcing your gateway to terminate the PPPoA connection. The advantage is that the PPPoA termination is done within the gateway and not on your PC; this frees up your PC resources and allows multiple users to utilize the PPPoA connection.

Follow the instructions below to configure the gateway as PPPoA.

1. From the Setup main page, click on **New Connection**.
   The default PPPoE connection setup is displayed.

2. At the Type field select **PPPoA**.
   The PPPoA connection setup page is displayed. The picture below illustrates a typical PPPoA configuration.



PPPoA Connection Setup

Name:
Type: PPPoA
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

PPP Settings

Encapsulation: ● LLC ○ VC
Username: username
Password: ****
Idle Timeout: 60 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1500 bytes
On Demand: □
Default Gateway: ☑
Debug: □

PVC Settings

PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs

3. Enter a unique name for the PPPoA connection in the **Name** field.
   The name must not have spaces and cannot begin with numbers.

4. Under **PPP Settings**, select the encapsulation type (LLC or VC).

Note: If you are not sure just use the default mode.

5. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

Note: Your DSL service provider or your ISP will supply these.

6. Select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

7. Click the **apply** button to complete the connection setup. This will temporarily save this connection.

8. To make the change permanent, click on **Save all settings** in the left menu.

9. For connection, click on **Connect**.

The PPP options include following settings:

Field	Description
Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two options are provided: **Logical Link Control** (LLC) and **Virtual Channel** (VC).
Username	Your user name for the PPPoA access; this is provided by your DSL service provider or your ISP
Password	The password for the PPPoA access; this is provided by your DSL service provider or your ISP
Idle Timeout	Specifies that PPPoA connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a **0** in this field.
Keep Alive	When on-demand option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a **0** in this field

Field	Description
Authentication	Three authentication options are available: a**uto, Challenge Handshake Authentication protocol** (CHAP), and **Password Authentication Protocol** (PAP).
MTU	Maximum Transmit Unit the DSL connection can transmit. It is a negotiated value that asks the provider to send packets of no more than n bytes. The maximum specified value is 1500 although some DSL/ISP providers require a larger value. The minimum MTU value is 128.
On-Demand	Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
Default Gateway	If checked, this connection becomes the default gateway to the Internet.
Debug	Enables PPPoA connection debugging facilities. You can read about debugging in the following text.
PPP UNnumbered	This is a special feature for telecommunication. It is used for assigning blocks of public addresses to the client and makes the PPP appear as pass-through.
LAN	The LAN field associated with the PPP UNunmbered field. The packets need to go through specific LAN when the PPP UNnumbered feature is activated.

The VLAN Settings include the options showed in following table:

Field	Description
Sharing	This is where you enable/disable sharing. The VLAN needs to be selected to create VLAN.
VLAN ID	VLAN Identification
Priority Bits	Priority is given to a VLAN connection from 0-7, 0 means highest priority.

The following table describes the options of the PVC Settings:

Field	Description
PVC	Permanent virtual circuit. A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed
VPI	Virtual path identifier
VCI	Virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. It is sometimes called virtual channel connection.
QoS	Quality of Service, a feature of data transmission that measures how accurately and how quickly a message or data is transferred from a source computer to a destination computer over a network. The three QoS options are: **Undefined Bit Rate** (UBR), **Constant Bit Rate** (CBR), and **Variable Bit Rate** (VBR).
PCR	Peak Cell Rate (in cells/sec) is the cell rate, which the source may never exceed.
SCR	Sustain Cell Rate
MBS	Maximum Burst Size - traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell rate.
CDVT	Cell Delay Variation Tolerance
Auto PVC	Auto Permanent Virtual Circuit, see PVC.

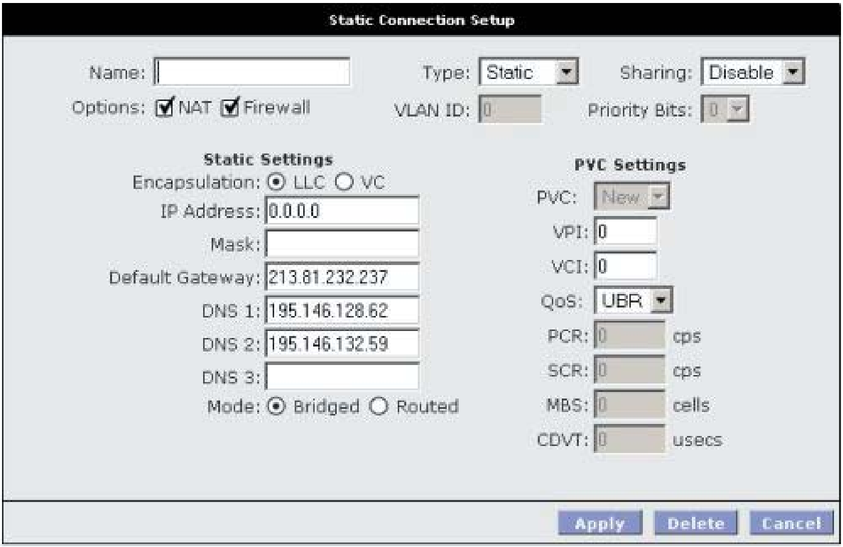
Static Connection Setup

Static is used whenever a known static IP is assigned. The accompanying information such as the Subnet mask and the gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers would enable you to have access to other web servers. Valid IP addresses range is from 0.0.0.0 to 255.255.255.255.

Use the following procedures to configure the gateway for a Static connection:

1. From the Setup main page, click on **New Connection**.
   The default PPPoE connection setup is displayed.

2. At the Type field select **Static**.
   The Static connection setup page is displayed. The picture below illustrates a typical Static configuration.



Static Connection Setup

Name:

Type: Static

Sharing: Disable

Options: ☑ NAT ☑ Firewall

VLAN ID: 0

Priority Bits: 0

Static Settings

Encapsulation: ● LLC ○ VC

IP Address: 0.0.0.0

Mask:

Default Gateway: 213.81.232.237

DNS 1: 195.146.128.62

DNS 2: 195.146.132.59

DNS 3:

Mode: ● Bridged ○ Routed

PVC Settings

PVC: New

VPI: 0

VCI: 0

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

CDVT: 0 usecs

3. Enter a unique name for the Static connection in the **Name** field.
   The name must not have spaces and cannot begin with numbers.

4. You can also enable Network Address Translation (NAT) and the Firewall options. If you are unsure, leave these in the default mode.

5. Under **Static settings**, select the **encapsulation** type (LLC or VC).

Note: If you are not sure just use the default mode.

6. Based upon the information your DSL/ISP provided, enter your assigned **IP address, Subnet Mask, Default Gateway** (if provided), and **Domain Name Services** (DNS) values (if provided).

7. For the static configuration, you can also select a **Bridged** connection or a **Routed** connection. Since static IP address is typically used to host WEB servers, you may want to use a bridge connection.

8. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

Note: Your DSL service provider or your ISP will supply these.

9. Select the **quality of service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.

10. Click the **apply** button to complete the connection setup. This will temporarily save this connection.

11. To make the change permanent, click on **Save all settings** in the left menu.

12. For connection, click on **Connect**.

The following table shows a description of the Static setting options:

Field	**Description**
Encapsulation	Two options are provided: **Logical Link Control** (LLC) and **Virtual Channel** (VC).
IP Address	IP address of the static connection.
Mask	Subnet mask provided by your ISP.
Gateway	Your gateways IP address.
Default Gateway	If checked, this connection becomes the default gateway to the Internet.
DNS	Domain Name Server address provided by your ISP.
Mode	The Bridged and Routed modes are available.

The VLAN Settings include the options showed in following table:

Field	**Description**
Sharing	This is where you enable/disable sharing. The VLAN needs to be selected to create VLAN.
VLAN ID	VLAN Identification
Priority Bits	Priority is given to a VLAN connection from 0-7, 0 means highest priority.

The following table describes the options of the PVC Settings:

Field	**Description**
PVC	Permanent virtual circuit. A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.
VPI	Virtual path identifier
VCI	Virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. It is sometimes called virtual channel connection.
QoS	Quality of Service, a feature of data transmission that measures how accurately and how quickly a message or data is transferred from a source computer to a destination computer over a network. The three QoS options are: **Undefined Bit Rate** (UBR), **Constant Bit Rate** (CBR), and **Variable Bit Rate** (VBR).
PCR	Peak Cell Rate (in cells/sec) is the cell rate, which the source may never exceed.
SCR	Sustain Cell Rate
MBS	Maximum Burst Size - traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell rate.
CDVT	Cell Delay Variation Tolerance
Auto PVC	Auto Permanent Virtual Circuit, see PVC.

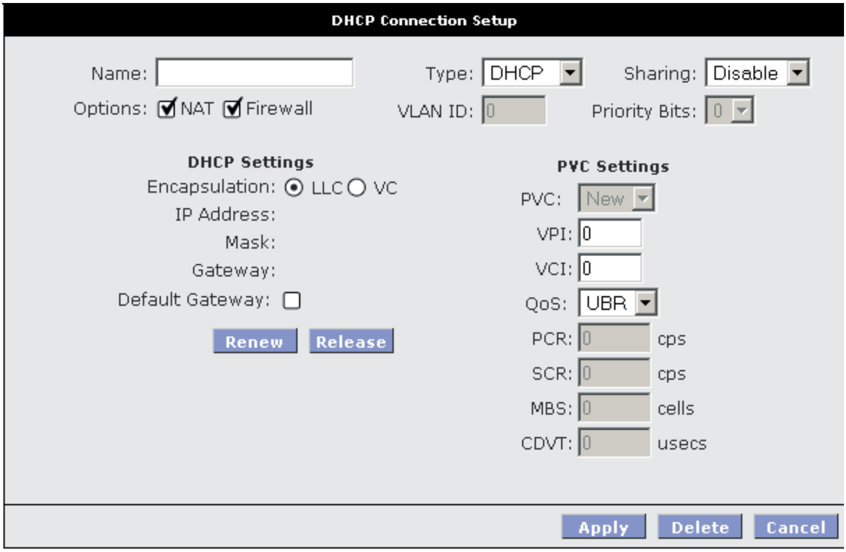
DHCP Connection Setup

Dynamic Host Configuration Protocol (DHCP) allows the gateway to automatically obtain the IP address from the server. This option is commonly used in situations where IP is dynamically assigned and is not known prior to assignment.

Use the following procedures to configure the gateway for a DHCP connection.

1. From the Setup main page, click on **New Connection**.
   The default PPPoE connection setup is displayed.

2. At the Type field select **DHCP**.
   The PPPoE connection setup page is displayed. The picture below illustrates a typical DHCP configuration.



DHCP Connection Setup

Name:
Type: DHCP
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

DHCP Settings
Encapsulation: ● LLC ○ VC
IP Address:
Mask:
Gateway:
Default Gateway: □

PVC Settings
PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs

3. If your DSL line is connected and your DSL/ISP provider is supporting DHCP, you can click the **Renew** button and the gateway will retrieve an IP address, Subnet mask, and Gateway address. At anytime, you can release the DHCP address by clicking on the **Release** button, and renew the DHCP address by clicking on the **Renew** button.

4. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

Note: Your DSL service provider or your ISP will supply these.

5. Select the **quality of service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.

6. Click the **apply** button to complete the connection setup. This will temporarily save this connection.

7. To make the change permanent, click on **Save all settings** in the left menu.

8. For connection, click on **Connect**.

The DHCP options are described in the following table:

Field	Description
Encapsulation	Two options are provided: **Logical Link Control** (LLC) and **Virtual Channel** (VC).
IP Address	IP address of the static connection.
Mask	Subnet mask provided by your ISP.
Gateway	Your gateways IP address.
Default Gateway	If checked, this connection becomes the default gateway to the Internet.

The VLAN Settings include the options showed in following table:

Field	Description
Sharing	This is where you enable/disable sharing. The VLAN needs to be selected to create VLAN.
VLAN ID	VLAN Identification
Priority Bits	Priority is given to a VLAN connection from 0-7, 0 means highest priority.

The following table describes the options of the PVC Settings:

Field	Description
PVC	Permanent virtual circuit. A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.
VPI	Virtual path identifier
VCI	Virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. It is sometimes called virtual channel connection.
QoS	Quality of Service, a feature of data transmission that measures how accurately and how quickly a message or data is transferred from a source computer to a destination computer over a network. The three QoS options are: **Undefined Bit Rate** (UBR), **Constant Bit Rate** (CBR), and **Variable Bit Rate** (VBR).

Field	Description
PCR	Peak Cell Rate (in cells/sec) is the cell rate, which the source may never exceed.
SCR	Sustain Cell Rate
MBS	Maximum Burst Size - traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell rate.
CDVT	Cell Delay Variation Tolerance
Auto PVC	Auto Permanent Virtual Circuit, see PVC.

Bridged gateway profile and Connection

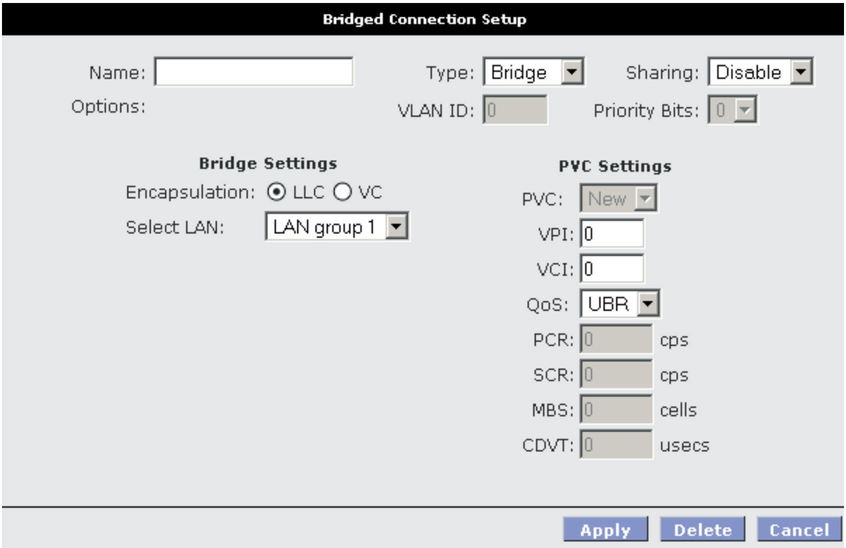
A pure bridged connection does not assign any IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method, as shown on next picture, makes the Gateway act as a hub, and just passes packets across the WAN interface to the LAN interface.

Use the following procedures to configure the gateway as a bridge.

1. From the Setup main page, click on **New Connection**.
   The default PPPoE connection setup is displayed.

2. At the Type field select **Bridge**.

3. The Bridge connection setup page is displayed.



Bridged Connection Setup

Name:
Type: Bridge
Sharing: Disable
Options:
VLAN ID: 0
Priority Bits: 0

Bridge Settings
Encapsulation: ● LLC ○ VC
Select LAN: LAN group 1

PVC Settings
PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs

4. Enter a unique name for the Bridge connection in the **Name** field. The name must not have spaces and cannot begin with numbers.

5. Under **Bridge Settings**, select the encapsulation type (LLC or VC). Note: If you are not sure just use the default mode.

6. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

Note: Your DSL service provider or your ISP will supply these.

7. Select the **quality of service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.

8. Click the **apply** button to complete the connection setup. This will temporarily save this connection.

9. To make the change permanent, click on **Save all settings** in the left menu.

10. For connection, click on **Connect**.

The Bridge Settings include the following options:

Field	Description
Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two options are provided: Logical Link Control (LLC) and Virtual Channel (VC).
Select LAN	There are three ethernet bridges you can select from.

The VLAN Settings include the options showed in following table:

Field	Description
Sharing	This is where you enable/disable sharing. The VLAN needs to be selected to create VLAN.
VLAN ID	VLAN Identification

Field	Description
Priority Bits	Priority is given to a VLAN connection from 0-7, 0 means highest priority.

The following table describes the options of the PVC Settings:

Field	Description
PVC	Permanent virtual circuit. A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.
VPI	Virtual path identifier
VCI	Virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. It is sometimes called virtual channel connection.
QoS	Quality of Service, a feature of data transmission that measures how accurately and how quickly a message or data is transferred from a source computer to a destination computer over a network. The three QoS options are: **Undefined Bit Rate** (UBR), **Constant Bit Rate** (CBR), and **Variable Bit Rate** (VBR).
PCR	Peak Cell Rate (in cells/sec) is the cell rate, which the source may never exceed.
SCR	Sustain Cell Rate
MBS	Maximum Burst Size - traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell rate.
CDVT	Cell Delay Variation Tolerance
Auto PVC	Auto Permanent Virtual Circuit, see PVC.

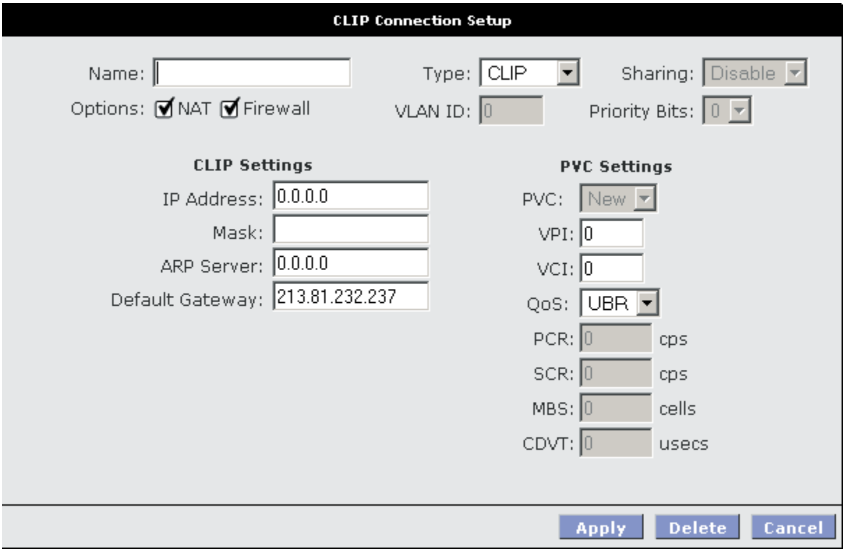
Classical IP over ATM (CLIP, defined in RFC1577) Connection Setup

The Classical IP over ATM (CLIP) support provides the ability to transmit IP packets over an ATM network, TI's CLIP support will encapsulate IP in an AAL5 packet data unit (PDU) frame using RFC1577 and it utilizes an ATM aware version of the ARP protocol (ATMARP). TI's CLIP support only allows PVC support; it does not support SVC.

Use the following procedures to configure the gateway for a CLIP connection.

1. From the Setup main page, click on **New Connection**.
   The default PPPoE connection setup is displayed.

2. At the Type field select **CLIP**.
   The CLIP connection setup page is displayed as shown below.



CLIP Connection Setup

Name:

Type: CLIP

Sharing: Disable

Options: ☑ NAT ☑ Firewall

VLAN ID: 0

Priority Bits: 0

CLIP Settings

IP Address: 0.0.0.0

Mask:

ARP Server: 0.0.0.0

Default Gateway: 213.81.232.237

PVC Settings

PVC: New

VPI: 0

VCI: 0

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

CDVT: 0 usecs

3. Enter a unique name for the Static connection in the **Name** field.
   The name must not have spaces and cannot begin with numbers.

4. You can also enable Network Address Translation (NAT) and the Firewall options.
   If you are unsure, leave these in the default mode.

5. Based upon the information your DSL/ISP provided, enter your assigned **IP address, Mask, ARP server,** and **Default Gateway**.

6. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

Note: Your DSL service provider or your ISP will supply these.

7. Select the **quality of service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.

8. Click the **Apply** button to complete the connection setup. This will temporarily save this connection.

9. To make the change permanent, click on **Save all settings** in the left menu.

10. For connection, click on **Connect**.

A description of the CLIP setting options is described in the following table:

Field	**Description**
IP Address	IP address of the CLIP connection provided by your ISP.
Mask	Subnet mask provided by your ISP.
ARP Server	Address Resolution Protocol (ARP) server
Default Gateway	If checked, this connection becomes the default gateway to the Internet.

The VLAN Settings include the options showed in following table:

Field	**Description**
Sharing	This is where you enable/disable sharing. The VLAN needs to be selected to create VLAN.
VLAN ID	VLAN Identification
Priority Bits	Priority is given to a VLAN connection from 0-7, 0 means highest priority.

The following table describes the options of the PVC Settings:

Field	**Description**
PVC	Permanent virtual circuit. A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.
VPI	Virtual path identifier
VCI	Virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. It is sometimes called virtual channel connection.

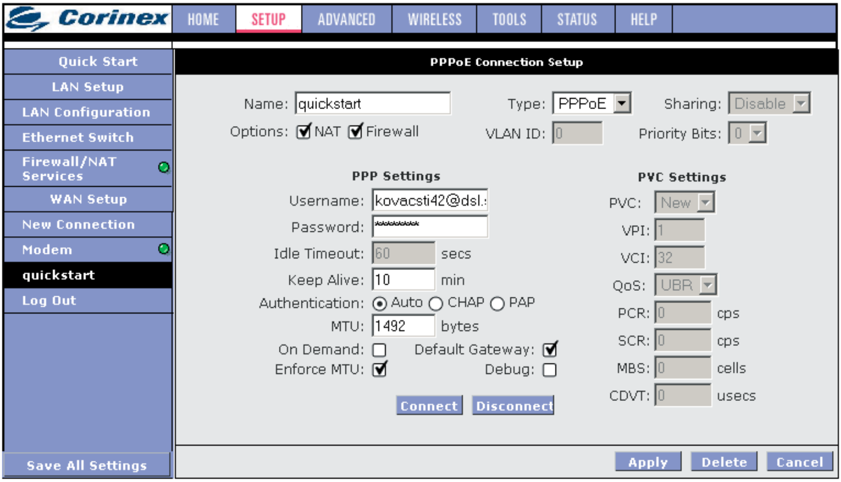
Field	Description
QoS	Quality of Service, a feature of data transmission that measures how accurately and how quickly a message or data is transferred from a source computer to a destination computer over a network. The three QoS options are: **Undefined Bit Rate** (UBR), **Constant Bit Rate** (CBR), and **Variable Bit Rate** (VBR).
PCR	Peak Cell Rate (in cells/sec) is the cell rate, which the source may never exceed.
SCR	Sustain Cell Rate
MBS	Maximum Burst Size - traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell rate.
CDVT	Cell Delay Variation Tolerance
Auto PVC	Auto Permanent Virtual Circuit, see PVC.

4.3.7 Modem

In this section you can set up modulation of your ADSL2+ modem. You can choose from MMODE, T1413, GDMT and GLITE. Please contact your provider in order to correctly configure your modem.

Active connections

Below the **Modem** section, you can see all created WAN connections. You can click on each on them to enter its configuration page. For example, in the picture below you can see configuration of the connection **Quickstart** which we created using the Quick Start connection wizard.



PPPoE Connection Setup

Name: quickstart Type: PPPoE Sharing: Disable

Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Username: kovacsti42@dsl.:

Password: ********

Idle Timeout: 60 secs

Keep Alive: 10 min

Authentication: ● Auto ○ CHAP ○ PAP

MTU: 1492 bytes

On Demand: □ Default Gateway: ☑

Enforce MTU: ☑ Debug: □

PVC Settings

PVC: New

VPI: 1

VCI: 32

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

CDVT: 0 usecs

Here you can see all the settings of the connection. You can review or edit all the settings. In case the chosen connection is currently used for communication, it has to be disconnected prior to making any changes.

Additionally, you can delete the connection by clicking on the **Delete** button.

4.4 Advanced Tab

The Advanced tab allows you to perform advanced configuration functions for existing connections including:

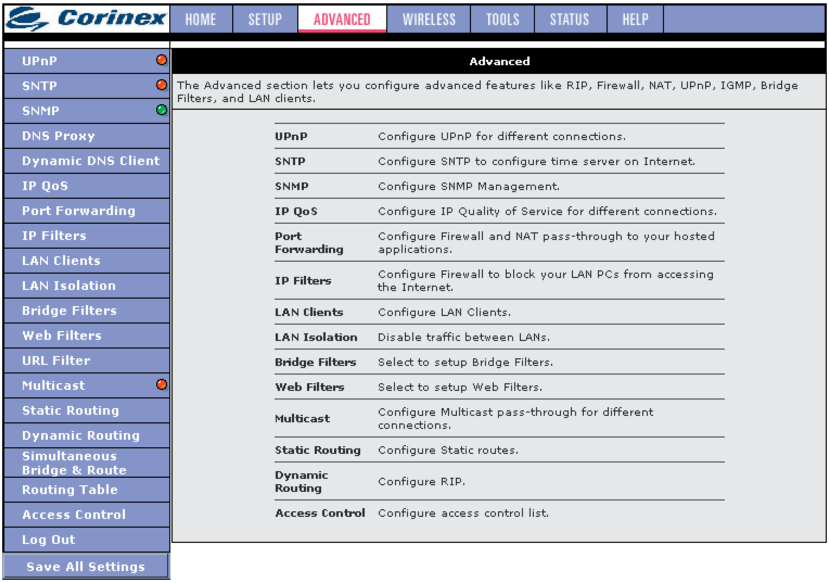
- Enabling and disabling of key features including voice, UPnP, SNTP, SNMP, IP QoS, RIP, access control, and multicasting
- Assigning IP QoS weighting
- Management of LAN port interfaces, packet flow, and filtering

Note: At least one WAN connection must be configured before implementing advanced WAN configuration features.

Note: At least one LAN group must be defined before implementing advanced LAN configuration features.

4.4.1 Main Screen

If you click on the **Advanced** tab, the following screen will open.



Advanced

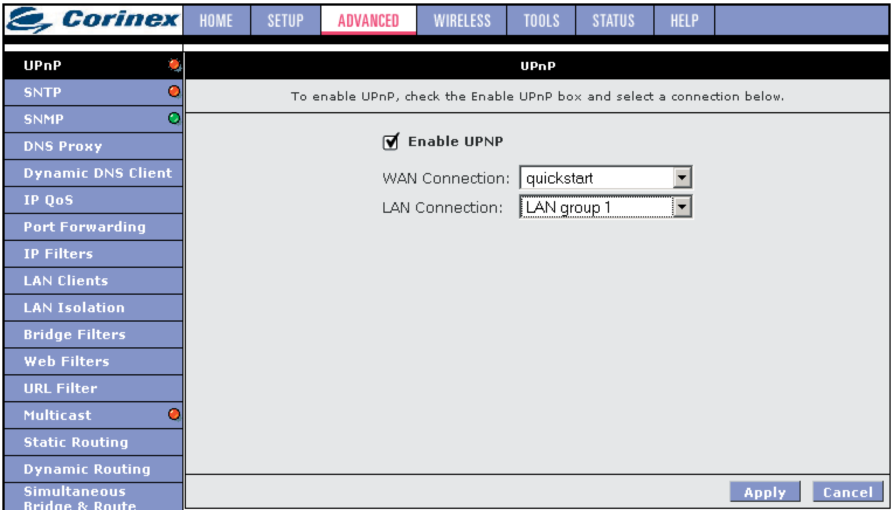
The Advanced section lets you configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, and LAN clients.

UPnP	Configure UPnP for different connections.
SNTP	Configure SNTP to configure time server on Internet.
SNMP	Configure SNMP Management.
IP QoS	Configure IP Quality of Service for different connections.
Port Forwarding	Configure Firewall and NAT pass-through to your hosted applications.
IP Filters	Configure Firewall to block your LAN PCs from accessing the Internet.
LAN Clients	Configure LAN Clients.
LAN Isolation	Disable traffic between LANs.
Bridge Filters	Select to setup Bridge Filters.
Web Filters	Select to setup Web Filters.
Multicast	Configure Multicast pass-through for different connections.
Static Routing	Configure Static routes.
Dynamic Routing	Configure RIP.
Access Control	Configure access control list.

Advanced features implemented in the *Corinex ADSL2+ Wireless Gateway G* include the following sections:

4.4.2 UPnP

UPnP (Universal Plug and Play), NAT (Network Address Translation) and Firewall Traversal allow traffic to pass through the Gateway for applications using the UPnP protocol. UPnP can be enabled/disabled across Multiple LAN segments. This feature requires one active DSL connection. In presence of multiple DSL connections, select the one over which the incoming traffic will be present, for example the default Internet connection.



UPnP

To enable UPnP, check the Enable UPnP box and select a connection below.

☑ Enable UPNP

WAN Connection: quickstart

LAN Connection: LAN group 1

Follow the steps below to enable UPnP.

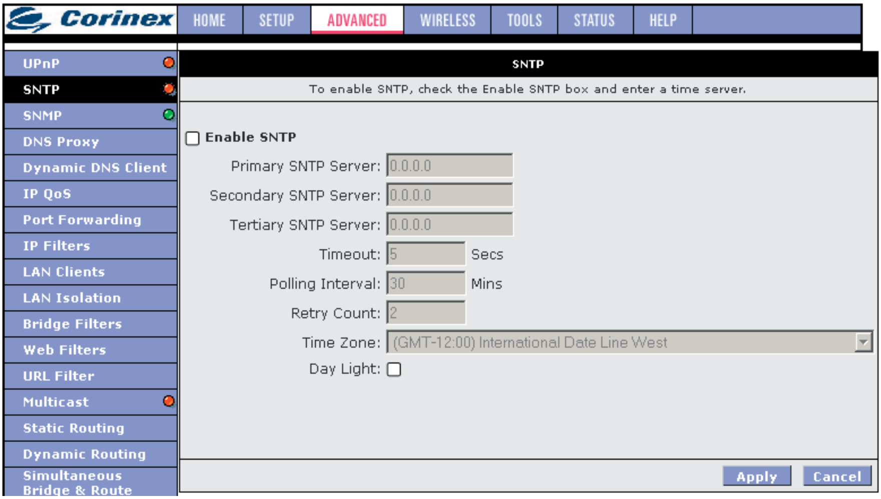
1. Check **Enable UPnP**. This enables the WAN Connection and LAN Connection fields.

2. Select the **WAN Connection** and **LAN Connection** from the drop-down lists.

3. Click **Apply**.

4.4.3 SNTP

SNTP (Simple Network Timing Protocol) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers. The following picture shows the default SNTP screen.



SNTP

To enable SNTP, check the Enable SNTP box and enter a time server.

□ Enable SNTP

Primary SNTP Server: 0.0.0.0

Secondary SNTP Server: 0.0.0.0

Tertiary SNTP Server: 0.0.0.0

Timeout: 5 Secs

Polling Interval: 30 Mins

Retry Count: 2

Time Zone: (GMT-12:00) International Date Line West

Day Light: □

When the SNTP feature is enabled, your Gateway will start querying for the time clock information from the primary SNTP server. If it fails to get a valid response within the "timeout" period, it will try for "retry" number of times, before moving to the Secondary SNTP server. If it fails to get a valid response from Secondary STNP server within valid retry times, it starts querying Tertiary SNTP server. If it fails to get a valid response from all the servers, then the program stops. When a valid response is received from one of the server, the program sleeps for **Polling Interval** amount of minutes, before starting the whole process again.

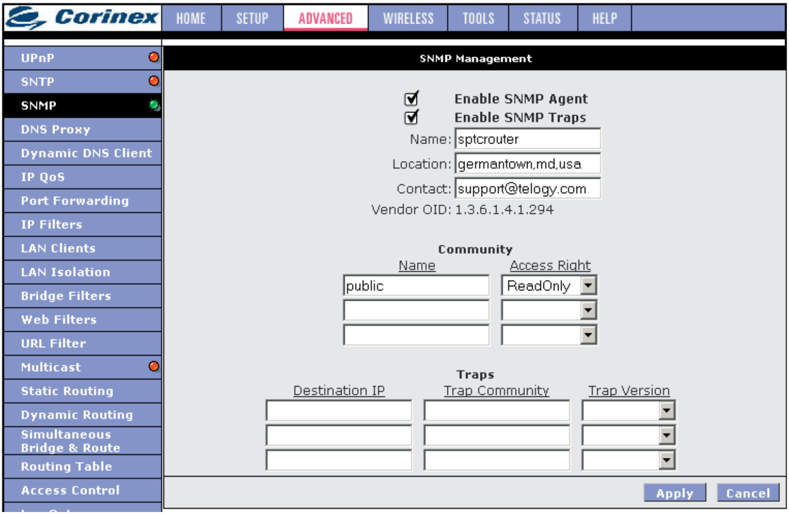
By default, SNTP is disabled. For enabling, check the **Enable SNTP** checkbox and fill the boxes according to the following table:

Field	Description
Primary SNTP Server	The IP address or the host name of the primary SNTP server.
Secondary SNTP Server	The IP address or the host name of the secondary SNTP server.
Tertiary SNTP Server	The IP address or the host name of the tertiary SNTP server.

Field	Description
Timeout	If the Gateway failed to connect to a SNTP server within the ‘Timeout’ period, it will retry the connection.
Polling Interval	Time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.
Retry count	The number of times the Gateway will try to connect to an SNTP server before it try to connect to the next server in line.
Time Zone	The time zone of the Gateway.
Day Light	Check/uncheck this option to enable/disable day light saving.

4.4.3 SNMP

SNMP (Simple Network Management Protocol) is a troubleshooting and management protocol, which uses the UDP protocol on port 161 to communicate between clients and servers. The following picture shows the default SNMP screen.



SNMP Management

☑ Enable SNMP Agent
☑ Enable SNMP Traps

Name: sptcrouter
Location: germantown,md,usa
Contact: support@telogy.com
Vendor OID: 1.3.6.1.4.1.294

Community

Name	Access Right
public	ReadOnly

Traps

Destination IP	Trap Community	Trap Version

SNMP uses a manager MIB (management information base) agent solution to fulfill the network management needs. The agent is a separate station that can request data from an SNMP agent in each of the different managed systems in the network. The agent uses the MIBs as dictionaries of manageable objects. Each SNMP-managed device has at least one agent that can respond to the queries from the NMS. The SNMP agent supports GETS, SETS, and TRAPS for 4 groups with MIB-II: System, Interface, IP, and ICMP.

The SNMP agents support 3 community names authentication.

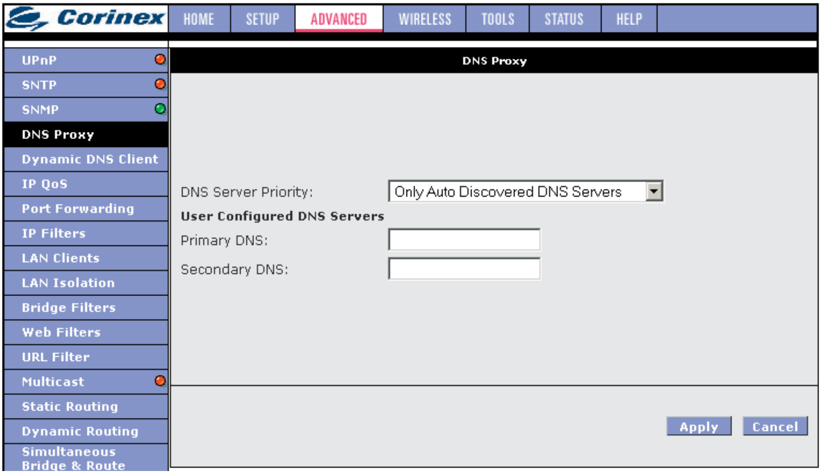
In the table below, you can find description of all fields in this section.

Field	Definition/ Description
Enable SNMP Agent	SNMP Agents are enabled by default.
Enable SNMP Traps	SNMP Traps are enabled by default.
Name	An administratively-assigned name for the gateway. By convention, this is the node's fully-qualified domain name.
Location	The physical location of the Gateway.
Contact	Contact person and/or contact information for the Gateway.
Vendor OID	Vendor object identifier. Private MIBs fit under OID 1.3.6.1.4.1. The enterprise number of TI is 294.
Community	SNMP defines a community to be a relationship between an SNMP agent and one or more SNMP managers. Once the clear-text community name corresponds to a community known to the receiving SNMP entity, the sending SNMP entity is considered to be authenticated as a member of that community and is granted different levels of access: read-only or read-write. The combination of community access mode and that of an object, a community profile is defined for each object. The community profile defines the operation permitted to the object. In the Linux NSP Gateway, a default community name of "public" with access mode of "read-only" is created in the configuration file. It allows a GET or a GETNEXT operation to all objects with access rights of READ-ONLY and READ-WRITE in the MIB..

Field	Definition/ Description
Community Name	Name of community. SNMP supports up to 3 communities including the default community name of "public".
Community Access Point	Two options are offered: • ReadOnly: Allows a GET or a GETNEXT operation to all objects with access rights of READ-ONLY in the MIB. • ReadWrite: Allows a GET or a GETNEXT operation to all objects with access rights of READ-WRITE in the MIB.
Trap	Trap is event notification. There are 4 standard traps supported in Linux Gateway: WarmStartTrap, LinkUpTrap, LinkDownTrap, and AuthenticationFailureTrap.
Trap Destination IP	Destination IP address of trap. Trap can be sent to 3 different destinations.
Trap Community	The SNMP Trap community string is used when sending SNMP Traps to another device. The community name functions as a password for sending trap notifications to the target SNMP manager
Trap Version	Two trap versions/formats are supported: •SNMP v1 •SNMP v2c

4.4.4 DNS Proxy

The Gateway can act as a DNS Proxy. A DNS proxy can take DNS queries from the local network and forward them to an Internet Domain Name Server. In this section you can configure two DNS servers which will be contacted with DNS queries.



DNS Proxy

DNS Server Priority: Only Auto Discovered DNS Servers

User Configured DNS Servers

Primary DNS:

Secondary DNS:

You can select the order for choosing DNS servers for queries in the field **DNS Server Priority** according to the following table.

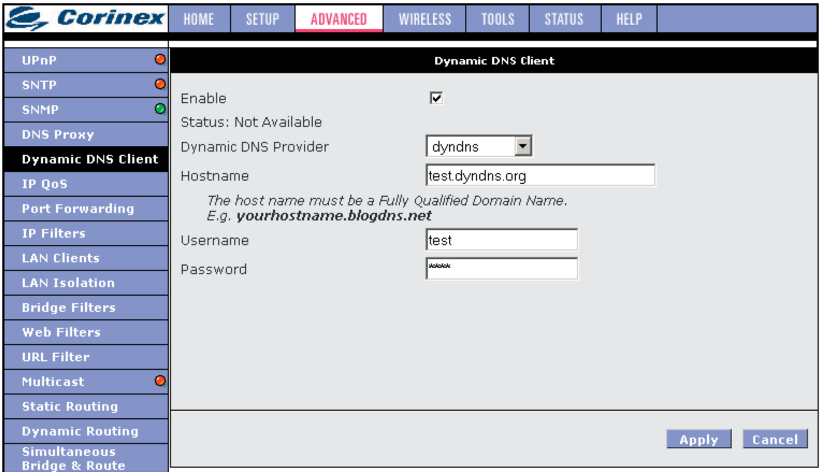
DNS Server Priority	Meaning
Only Auto Discovered DNS Servers	Usually the provider sends the DNS server settings to the gateway.
Only User Configured DNS Servers	With this setting only the automatically detected DNS servers will be used for DNS queries.
Only User Configured DNS Servers	If the provider didn't send any DNS settings to the gateway, or you prefer other DNS servers, you can enable DNS requests only to user configured DNS servers.
Auto Discovered then User Configured	The queries will be sent to all DNS servers and auto discovered DNS servers will be preferred.
User Configured then Auto Discovered.	The queries will be sent to all DNS servers and user configured DNS servers will be preferred.

Additionally, you can enter two DNS servers as the **user configured DNS servers**.

4.4.5 Dynamic DNS Client

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in many domains offered from DynDNS providers, allowing your computer to be more easily accessed from various locations on the Internet.

The Dynamic DNS service is ideal for a home website, file server, or just to keep a pointer back to your home PC so you can access those important documents while you're at work. Using the DynDNS client in the Gateway, you can keep your hostname always pointing to your IP address, no matter how often your ISP changes it.



Dynamic DNS Client

Enable ☑

Status: Not Available

Dynamic DNS Provider: dyndns

Hostname: test.dyndns.org

The host name must be a Fully Qualified Domain Name.
E.g. ***yourhostname.blogdns.net***

Username: test

Password: ****

In this screen you can select the following options.

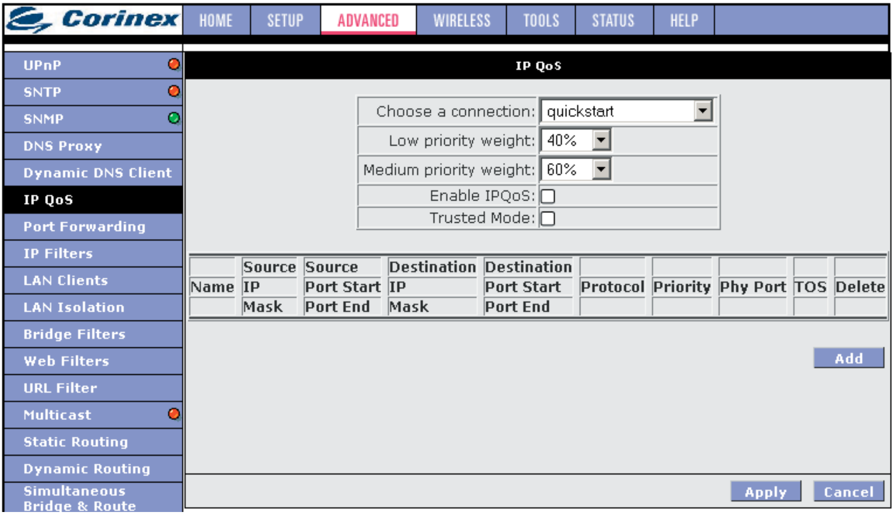
Field	**Definition/ Description**
Enable	With this checkbox you can enable or disable the DynDNS client in the Gateway.
Status	This field shows the current status of your DynDNS domain.
Dynamic DNS Provider	You can select one of the most used DynDNS providers, where you have your DynDNS account.
Hostname	In this field, please enter the full name of your registered DynDNS domain.

Field	Definition/ Description
Username	In this field please enter your DynDNS username
Password	In this field please enter your DynDNS password.

After setting up, please click on **Apply**.

4.4.6 IP QoS

When QoS is enabled in the Gateway, the designated machine, application or person would have precedence over peers when competing for bandwidth. The IP QoS Setup page allows you to configure QoS for a connection, view previously configured QoS rules, add a new rule, or delete an existing rule.



IP QoS

Choose a connection:	quickstart
Low priority weight:	40%
Medium priority weight:	60%
Enable IPQoS:	□
Trusted Mode:	□

Name	Source IP Mask	Source Port Start Port End	Destination IP Mask	Destination Port Start Port End	Protocol	Priority	Phy Port	TOS	Delete

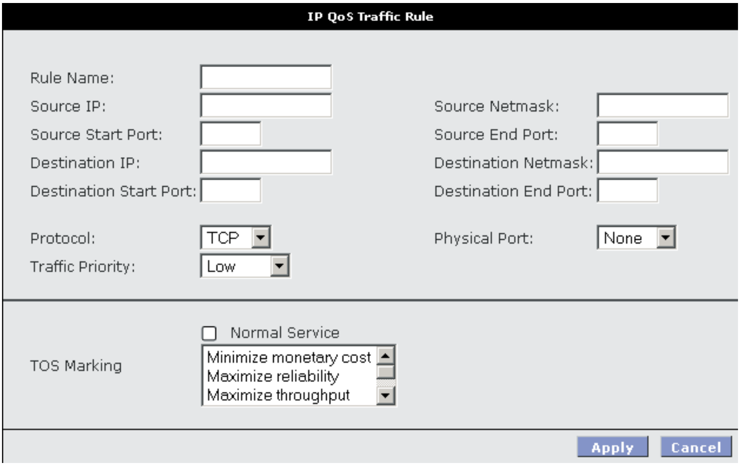
Each output device has three priority queues associated with transmit data. The high priority queues have strict priority over the medium priority and low priority queues, and therefore can exhaust all available bandwidth. The web UI will allow the user to select the weights of the medium and low priority queues in increments of 10 percent so that that the sum of the weights of the 2 queues is equal to 100 percent. These queues will be serviced on a Round Robin priority basis according to the weights assigned, after the high priority queues have been completely serviced.

In the following table, you can find a description of all settings in this screen.

Field	**Definition/ Description**
Choose a connection	This field allows you choose a connection from the list of available connections. For example choose a WAN connection to enable IP QoS for the Upstream traffic of the Modem. On the other hand choose the LAN connection (Ethernet and USB Bridged) for the downstream traffic.
Low Priority weight Medium priority weight	These 2 fields will allow you to select the weights of the Medium and Low priority queues in increments of 10 percent, so that that the sum of the weights of these 2 queues is equal to 100 percent.
Enable IPQoS	This field allows you to enable/disable IP QoS for the chosen connection. **Note**: If IP QoS is enabled and no rules are defined, a default rule is applied to the connection. The default rule puts all the traffic to be transmitted in the Low Priority queue
Trusted Mode	The NSP has two primary modes of operation with regard to queue traffic prioritization - Trusted and Un-trusted. This field allows you to choose the mode - Trusted (checked) and Un-trusted (Unchecked). In **Trusted mode** all the rules will be applied first, regardless of the setting of the TOS bits. After the rules have been exhausted the existing TOS bit settings will be honored. The **Un-trusted** mode will match first against all rules as in Trusted mode. The difference is that if there is no match then a default rule will be used. The default rule will have an associated queuing priority - Low.

In case you enabled the IP QoS field, you can add detailed rules for QoS.

For adding a rule, please select the connection from the **choose a connection** list and click **Add**. The following screen will appear:



IP QoS Traffic Rule

Rule Name:			
Source IP:		Source Netmask:	
Source Start Port:		Source End Port:	
Destination IP:		Destination Netmask:	
Destination Start Port:		Destination End Port:	
Protocol:	TCP	Physical Port:	None
Traffic Priority:	Low		

TOS Marking

□ Normal Service

Minimize monetary cost
Maximize reliability
Maximize throughput

The Rules configuration page will allow you to define IP matching fields to associate with the priority queues associated with the named connections selected above in the “QoS Setup Page” section.

There will be three primary fields for you to select:

- A Trusted mode check box.
- A traffic priority choice (EF2/High, Medium, Low). Note that EF1 is not a choice for the user as it is meant only for voice control packets.
- An IP rules matching selection area.

The Gateway has two primary modes of operation with regard to queue traffic prioritization: Trusted and Un-trusted. The Web UI will provide one check box to enable trusted mode. In **Trusted mode** all rules will be applied first, regardless of the setting of the TOS bits. After the rules have been exhausted the existing TOS bit settings will be honored. If the Trusted mode box is unchecked this will indicate the Un-trusted mode. **Un-trusted** mode will match first against all rules as in Trusted mode. The difference is that if there is no match then a default rule will be used. The default rule will have an associated queuing priority - Low.

Rule definitions will be defined by the user, by allowing the user to select matching based on Source IP and Netmask, Destination IP and Netmask, IP Protocol, Source Port range, Destination Port range, and Incoming Mac Port (switched LAN Port). These selections will define a rule and be associated with a particular queue priority: High, Medium, and Low. There is another option to choose a particular TOS marking. The allowed options are - No change, Normal service, Minimize monitory cost, Maximize reliability, Maximize throughput and Minimize delay.

In the following table you can find description of the IP QoS Traffic Rule Screen settings.

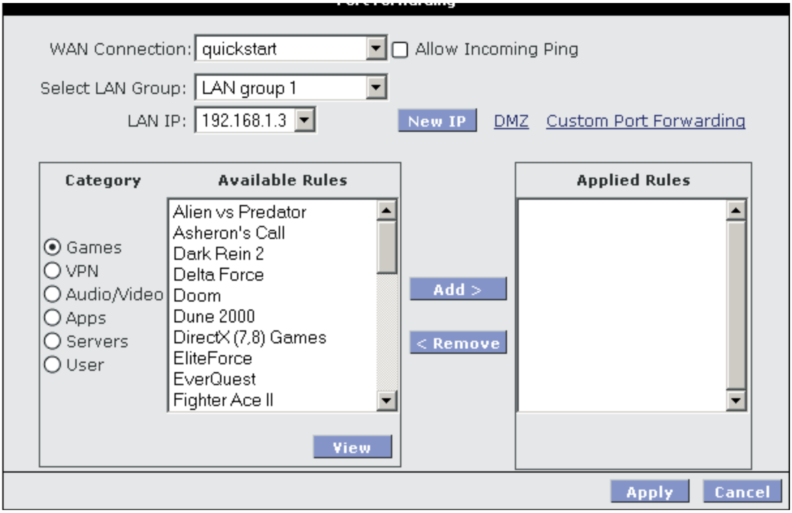
Field	Definition/ Description
Rule Name	Name of the traffic rule.
Source IP	The IP address of the traffic source.
Source Netmask	The netmask of the source.
Source Start Port	The start port of the source.
Source End Port	The end port of the source.
Destination IP	The IP address of the traffic destination.
Destination Netmask	The netmask of the destination.
Destination Start Port	The start port of the destination.
Destination End Port	The end port of the destination.
Protocol	The selections are TCP, UDP, ICMP, and any.
Physical Port	The selections are none, Port 1 through 4, USB, and WLAN.
Traffic Priority	The Traffic Priority field corresponds to the Priority Queue (High/Medium/Low) for this traffic. The possible options for Protocol are: ANY, ICMP, TCP, and UDP. Wildcard(*) entries are allowed for IP Address/Netmask and Port range fields .
Normal Service	Standard settings for TOS values.
TOS Marking	The TOS marking field allows you to assign a TOS value to this traffic. The values for the TOS marking can be: No Change, Normal Service, Minimize monetary cost, Maximize reliability, Maximize throughput, and Minimize delay.

After setting up a rule, please click on **Apply**.
If you want to delete a rule, check the checkbox **Delete** next to the rule and click **Apply**.

4.4.7 Port Forwarding

Port Forwarding (or Virtual Server) allows you to direct incoming traffic to specific PCs based on a service port number and protocol. Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. Port Forwarding is configurable per LAN segment.

A database of predefined Port Forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category, and add the available rules for a given category. You can also create/edit/delete your own Port Forwarding rules.



WAN Connection: quickstart □ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.3

Category: ● Games ○ VPN ○ Audio/Video ○ Apps ○ Servers ○ User

Field	Definition/ Description
WAN Connection	Select the WAN connection you are going to apply the port forwarding feature.
Select LAN Group	Select the LAN Group you are going to apply the port forwarding feature.
LAN IP	Select the IP address that will host the service.
Allow Incoming Ping	Enabling incoming ping (ICMP) requests on the Port Forwarding page allows the router to respond to a ping from the Internet.
DMZ	Demilitarized Zone. More information on DMZ is available later in this guide.
Custom Port Forwarding	This link takes you to the Custom Port Forwarding screen, which will be described later.
Category	Custom and user-defined categories.

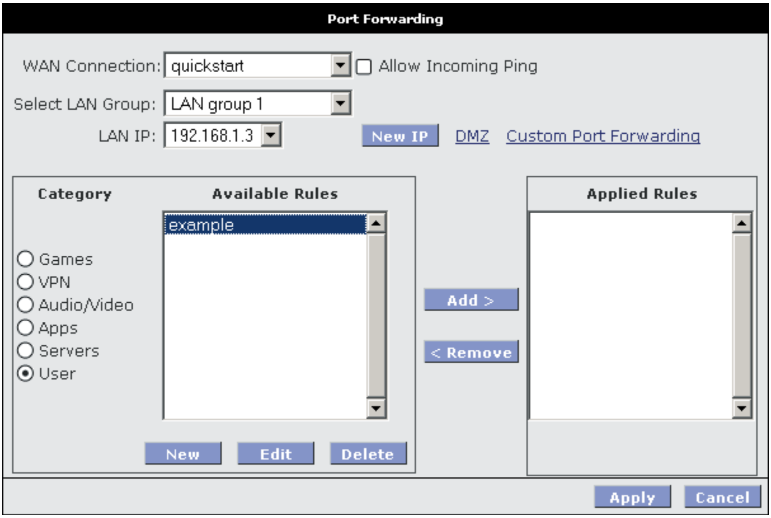
Field	Description
Available Rules	Predefined and/or user-defined IP filtering rules for each category.
Applied Rules	The IP filtering rules you selected to apply for each given category.

You can use the pre-configured entry for a LAN segment using the following procedure.

1. From the Port Forwarding configuration screen, select **WAN Connection, LAN Group,** and **LAN IP.** If the desired LAN IP is not available in the LAN IP drop-down menu, you can add it using the LAN Client screen, which can be accessed by clicking **NEW IP** .

2. Select the available rules for a given category, click **View** to view the rule associated with a predefined filter, click **Add** to apply the rule for this category.

3. If a rule is not in the list, you can create your own in the user category. With User category selected, click on **New**.



Port Forwarding

WAN Connection: quickstart ☐ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.3

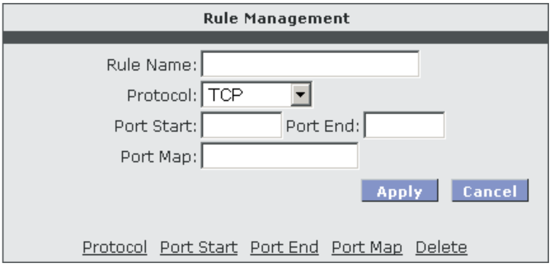
Category

○ Games
○ VPN
○ Audio/Video
○ Apps
○ Servers
● User

Available Rules: example

Applied Rules

The following window will appear, where you can create your own port forwarding rules:



Rule Management

Rule Name:

Protocol: TCP

Port Start: Port End:

Port Map:

The rule(s) you create will be available in the User category. You will be able to Edit/Delete the rule(s) you create.

4. Repeat adding rules to each category.

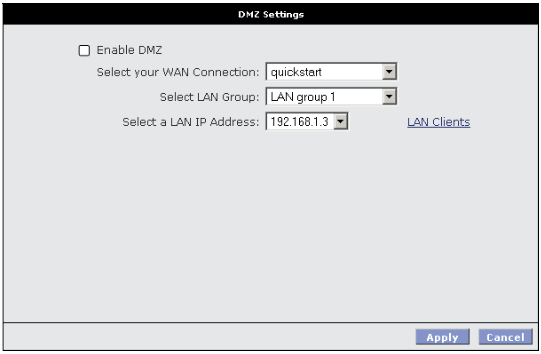
5. Click **Apply** when you finish.

4.4.8 DMZ Settings

Setting a computer on your local network as DMZ (DeMilitarized Zone) forwards any network traffic that is not redirected to another computer via the port forwarding feature to the computer's IP address. This opens the access to the DMZ computer from the Internet.

The DMZ function is disabled by default. Use the following procedures to enable it.

1. From the Port Forwarding configuration screen, click the DMZ link. You will be taken to the DMZ settings screen.



DMZ Settings

□ Enable DMZ

Select your WAN Connection: quickstart

Select LAN Group: LAN group 1

Select a LAN IP Address: 192.168.1.3

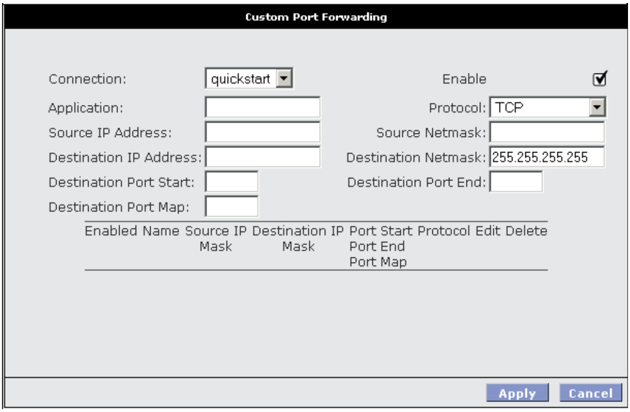
In the table below you can see the description of this screen.

Field	Description
Enable DMZ	Enable/disables the Demilitarized Zone feature. This field is unchecked by default.
Select your WAN Connection	Select the WAN Group you are going to apply the DMZ feature.
Select LAN Group	Select the LAN Group you are going to apply the DMZ feature.
Select a LAN IP Address	Select the LAN IP address you are going to use as the DMZ host. This computer will be exposed to the Internet. Be aware that this feature may expose your local network to security risks.
LAN Clients	This link will take you to the LAN Clients screen.

2. Check the **Enable DMZ** box on the DMZ setting screen.
3. Select the **WAN Group**, **LAN Group**, and **LAN IP Address**. DMZ is configurable per LAN segment.
4. Click **Apply** to enable the DMZ.

4.4.9 Custom Port Forwarding

The Custom Port Forwarding screen allows you to create up to 20 custom port forwarding entries to support specific services or applications; such as Concurrent NAT/NAPT operation.



Custom Port Forwarding

Connection:	quickstart	Enable	☑
Application:		Protocol:	TCP
Source IP Address:		Source Netmask:	
Destination IP Address:		Destination Netmask:	255.255.255.255
Destination Port Start:		Destination Port End:	
Destination Port Map:			

Enabled	Name	Source IP Mask	Destination IP Mask	Port Start Port End Port Map	Protocol	Edit	Delete

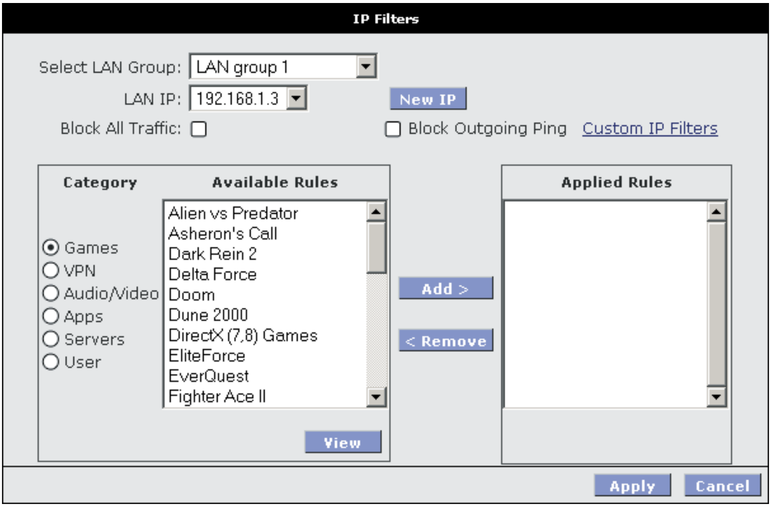
In the table below you can find a description on all settings in this screen.

Field	**Description**
Connection	Select the WAN connection you are going to apply the custom Port Forwarding rule.
Enable	The Enable button is checked by default, meaning this rule is applied when you click on the Apply button.
Application	Name of the application your port(s) will be opened for.
Protocol	There are three options available: **TCP, UDP**, and **TCP and UDP**.
Source IP Address	You can define the source IP address from which the incoming traffic will be allowed. Enter “0.0.0.0” for all.
Source Netmask	Netmask of the source IP address. Enter “255.255.255.255” for all.
Destination IP Address	Since it is for incoming traffic, the destination IP address is on your LAN side.
Destination Netmask	The destination netmask on your LAN side.
Destination Port Start	The starting port number that will be made open for this application.
Destination Port End	The ending port number that will be made open for this application.

4.4.10 IP Filters

The IP Filtering feature allows you to block specific applications/services based on the IP address of a LAN device. You can use this page to block specific traffic (for example block web access) or any traffic from a computer on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter, and add the available rules for a given category. You can also create/edit/delete your own IP filter rules.



IP Filters

Select LAN Group: LAN group 1

LAN IP: 192.168.1.3

Block All Traffic: □

□ Block Outgoing Ping

Category: ● Games ○ VPN ○ Audio/Video ○ Apps ○ Servers ○ User

Available Rules: Alien vs Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirectX (7,8) Games, EliteForce, EverQuest, Fighter Ace II

Applied Rules:

The table below describes the IP Filters screen.

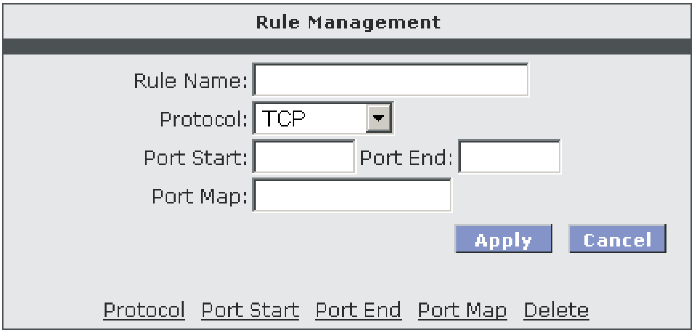
Field	Description
Select LAN Group	Select the LAN Group you are going to apply the IP Filters feature.
LAN IP	Select the IP address in the given LAN group that you are going to apply the IP Filters feature.
Block All Traffic	When checked, complete network access is blocked for the specific IP address.
Block Outgoing Ping	Blocking outgoing ping (ICMP) generated from a particular LAN IP can be used if your PC has a virus that attempts a Ping-of-Death Denial of Service attack.
Custom IP Filters	This link takes you to the Custom IP Filter screen, described later.
Available Rules	Predefined and/or user-defined IP filtering rules for each category.
Applied Rules	The IP filtering rules you selected to apply for each given category.

You can use the pre-configured entry for a LAN segment using the following procedure.

1. From the IP Filters configuration screen, select **LAN Group** and **LAN IP**. If the desired LAN IP is not available in the LAN IP drop-down menu, you can add it using the LAN Client screen, which can be accessed by clicking **NEW IP** .

2. Select the available rules for a given category, click **View** to view the rule associated with a predefined filter, click **Add** to apply the rule for this category.

3. If a rule is not in the list, you can create your own in the user category. Select User as category and click **Add**. The Rule Management screen will open.



Rule Management

Rule Name:

Protocol: TCP

Port Start: Port End:

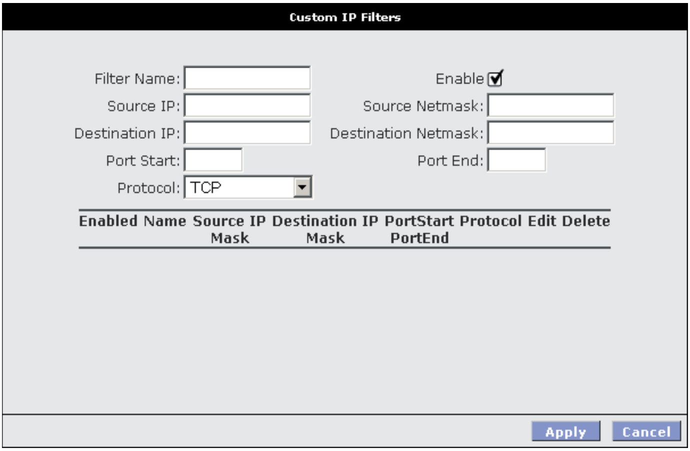
Port Map:

The rule(s) you create will be available in the User category. You will be able to Edit/Delete the rule(s) you create.

4. Repeat adding rules for each category.
5. Click **Apply**.

4.4.11 Custom IP Filters Screen

In the IP Filters screen, you can click on **Custom IP Filters** button to open the following page.



Custom IP Filters

Filter Name:		Enable	☑
Source IP:		Source Netmask:	
Destination IP:		Destination Netmask:	
Port Start:		Port End:	
Protocol:	TCP		

Enabled	Name	Source IP Mask	Destination IP Mask	PortStart PortEnd	Protocol	Edit	Delete

The Custom IP Filters function allows creation of up to 20 custom IP filtering entries to block specific services or applications based on:

- Source/Destination IP address and Netmask
- TCP Port (ranges supported)
- Protocol:
  - TCP
  - UDP
  - TCP and UDP
  - ICMP
  - Any

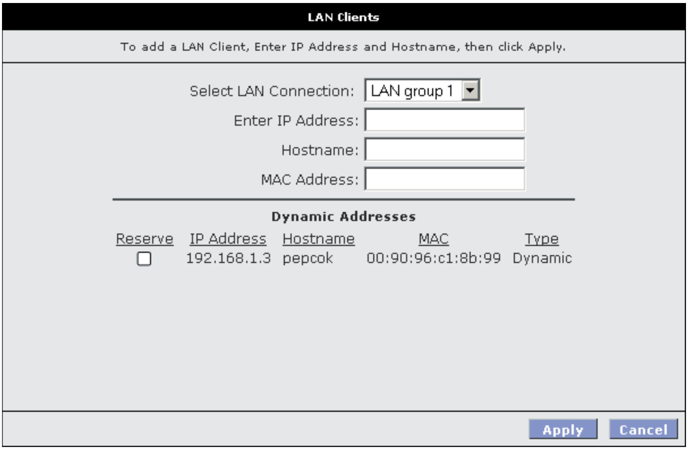
In the table below you can find the description of the Custom IP Filters page.

Field	Description
Filter Name	Name of the IP filter rule you are about to create.
Enable	The Enable button is checked by default, meaning this rule is applied when you click on the **Apply** button
Source IP	Since IP filtering is for outgoing traffic, the source IP is the IP address on your LAN side that you want to block network traffic from.
Source Netmask	Netmask of the source IP on your LAN side.
Destination IP	You can define the destination IP address to which your source IP will be banned the access. Enter “0.0.0.0” for all.

Field	Description
Destination Netmask	Netmask of the destination IP. Enter “255.255.255.255” for all.
Port Stat	The starting port number that will be blocked for this application.
Port End	The ending port number that will be blocked for this application.
Protocol	There are five options available: **TCP, UDP, TCP and UDP, ICMP**, and **Any**.

4.4.12 LAN Clients

The LAN Clients feature allows you to see all the PCs on the LAN segment. Each PC is qualified to be either **dynamic** (PC obtained a lease from this router) or **static** (PC has a manually configured IP address).



LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

Dynamic Addresses

Reserve	IP Address	Hostname	MAC	Type
□	192.168.1.3	pepcok	00:90:96:c1:8b:99	Dynamic

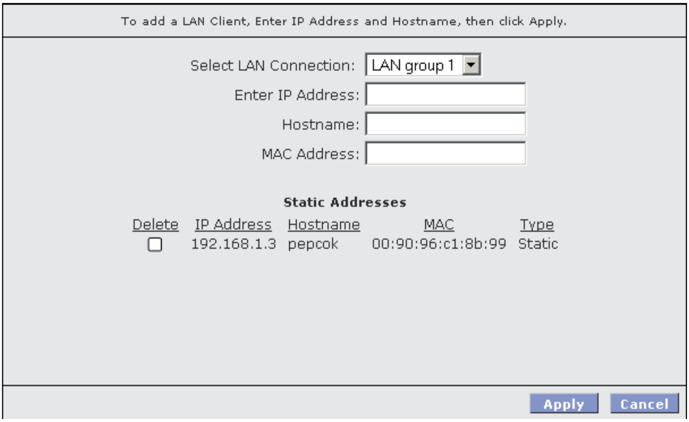
You can add a static IP address (belonging to the network segment of the router LAN IP address). Any existing static entry falling within DHCP server’s range can be deleted and the IP address would be made available for future allocation.
You can configure a LAN client using the following procedure.

1. From the LAN Clients screen, select **LAN Connection**, and enter **IP Address**, **Hostname**, and **MAC Address** according to the table below.

Field	Description
Select LAN Connection	Select the LAN connection you want to add the client to.
Enter IP Address	Assign the dynamic IP address to the PC here.
Hostname	Hostname of the client.
MAC Address	MAC address of the PC.

2. Click **Apply**. The IP address is now allocated and it shows up in the list of LAN clients as a dynamic entry

3. You can convert the dynamic entry into static by clicking **Reserve**, then **Apply.** As shown in the picture below, the IP is now changed to static address.



To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

Static Addresses

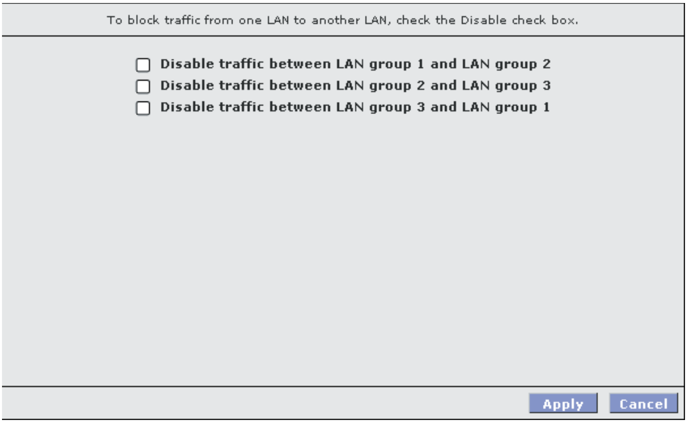
Delete	IP Address	Hostname	MAC	Type
□	192.168.1.3	pepcok	00:90:96:c1:8b:99	Static

You can delete this entry using the **Delete** checkbox.

Note: Changes applied to a static IP address will stay after the session is ended. Changes applied to a dynamic IP address will expire after the session is ended.

4.4.13 LAN Isolation

LAN isolation allows you to disable the flow of packets between up to three-user-defined LAN groups (WLAN, USB, and Ethernet). This allows you to secure information in private portions of the LAN from other, publicly accessible LAN segments.



To block traffic from one LAN to another LAN, check the Disable check box.

□ Disable traffic between LAN group 1 and LAN group 2
□ Disable traffic between LAN group 2 and LAN group 3
□ Disable traffic between LAN group 3 and LAN group 1

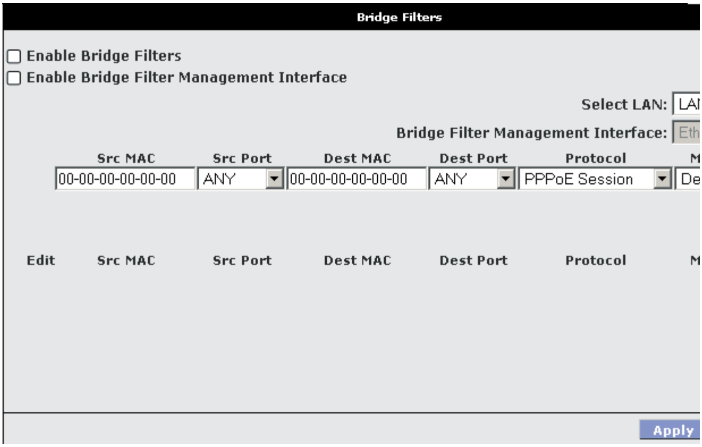
Follow the steps below to set up LAN isolation.

1. Check the traffic between the two LAN groups that you want to disable the packets flow.

2. Click **Apply**.

4.4.14 LAN Bridge Filters

The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against each defined filter rules sequentially. When a match is determined, the appropriate filtering action (either allow or deny) is performed. Please note that the bridge filter will only examine frames from interfaces which are part of the bridge itself. Twenty filter rules are supported with bridge filtering.



Bridge Filters

□ Enable Bridge Filters

□ Enable Bridge Filter Management Interface

Select LAN: LAN

Bridge Filter Management Interface: Eth

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	M
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	De

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	M

The User Interface for Bridge Filter allows you to enable/add/edit/delete the filter rules. Up to 20 entries are supported.

Follow the steps below to enable and configure Bridge Filters.

1. Check **Enable Bridge Filters**.

2. To add a rule, enter source MAC address, destination MAC address and frame type with desired filtering type, and click **Add**. You can also edit a rule that you created using the Edit checkbox. You can delete a rule using **Delete**.

3. Click **Apply**.

Note: There are three hidden filter rules within the bridge filter table. These rules are entered automatically by the system to ensure the user does not “lock” themselves out of the system. The first rule allows any and all ARP frames through the system. The second rule allows all IPv4 frames with the destination MAC address of the bridge to go through. The third rule allows all IPv4 frames with the source MAC address of the bridge to go through.

Please find the description of the options in this page, in the table below.

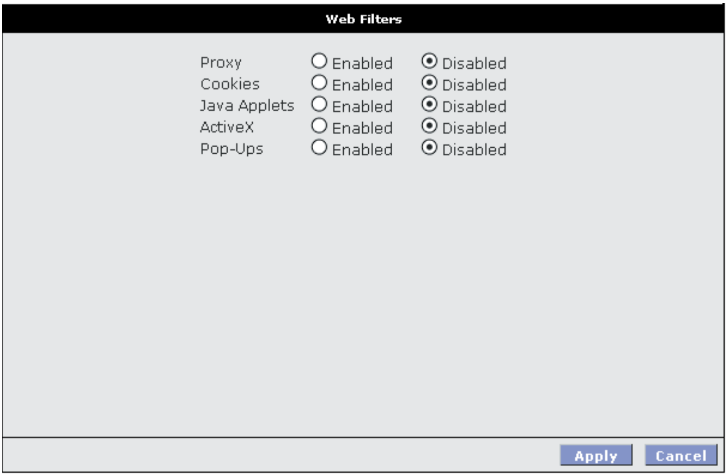
Field	Description
Enable Bridge Filters	Enable Bridge Filters button allow the user to enable or disable bridge filtering. It can be set/unset during any add/edit/delete operation. It can also be set/unset independently by just pressing the **Apply** button.
Enable Bridge Filter Management Interface	When checked, it enables the Bridge Filter Management Interface field.
Select LAN	Select your LAN group.
Bridge Filter Management Interface	You can choose from Ethernet, USB, and WLAN. .
SRC MAC	The source MAC address. It must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as "don't care". Blanks can be used in the MAC address space, and would be considered also as "don't care".
SRC Port	Source port. You can choose from Any, Ethernet, USB, and WLAN.
Dest MAC	The destination MAC address.
Dest Port	Destination port. You can choose from Any, Ethernet, USB, and WLAN.
Protocol	You can choose from the following options: PPPoE Session, PPPoE Discovery, IPX - Ethernet II, RARP, IPv6, IPv4, and Any.
Mode	There are two modes: **Deny** and **Allow**.

4.4.15 Web Filters

Web Filters allow you to manage the type of web content that passes through your gateway.
The following content types are disabled by default:

- Proxy Server
- Cookies
- Java Applets
- ActiveX Controls
- Pop-Ups

To enable, simply check **Enabled**, then click **Apply.**

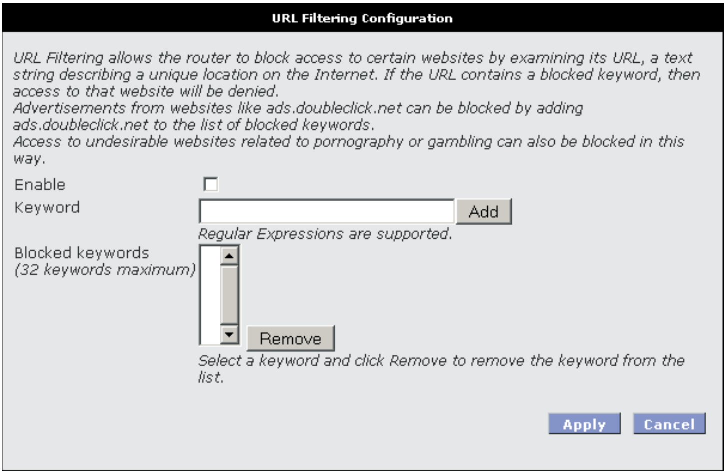


Web Filters

Proxy	○ Enabled	● Disabled
Cookies	○ Enabled	● Disabled
Java Applets	○ Enabled	● Disabled
ActiveX	○ Enabled	● Disabled
Pop-Ups	○ Enabled	● Disabled

4.4.16 URL Filter

URL Filtering allows the router to block access to certain websites by examining its URL, a text string describing a unique location on the Internet. If the URL contains a blocked keyword, then access to that website will be denied.



URL Filtering Configuration

URL Filtering allows the router to block access to certain websites by examining its URL, a text string describing a unique location on the Internet. If the URL contains a blocked keyword, then access to that website will be denied.
Advertisements from websites like ads.doubleclick.net can be blocked by adding ads.doubleclick.net to the list of blocked keywords.
Access to undesirable websites related to pornography or gambling can also be blocked in this way.

Enable □

Keyword

Regular Expressions are supported.

Blocked keywords
(32 keywords maximum)

Select a keyword and click Remove to remove the keyword from the list.

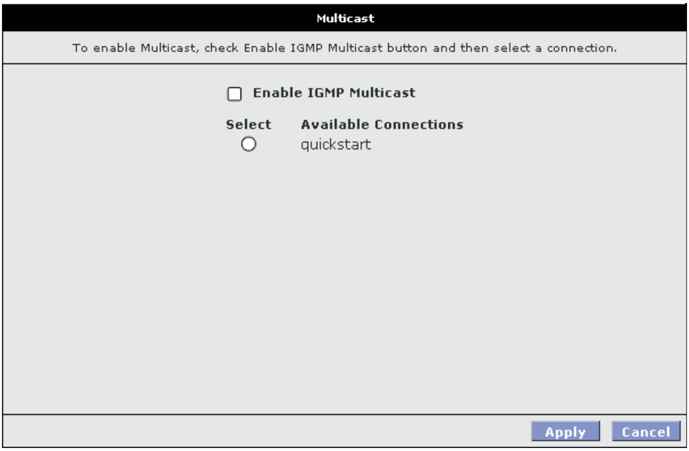
In the table below, find the description of the fields on this page.

Field	Description
Enable	You can either enable or disable the URL filtering.
Keyword	In this field you can enter the keyword for blocking. Any website address containing this keyword will be blocked. For example, if you want to block advertisements from websites like www.corinex.com, enter www.corinex.com into this field and click **Add**.
Blocked Keywords	This is a list of all blocked keywords. If you want to remove a keyword from the list, select it and click on **Remove**.

After adding or deleting keywords from the list, click **Apply**.

4.4.17 Multicasts

The Gateway supports an IGMP (Internet Group Management Protocol) proxy that handles IGMP messages. When enabled, the router will act as a proxy for a PC making requests for leaves and joins to multicast groups.



Multicast

To enable Multicast, check Enable IGMP Multicast button and then select a connection.

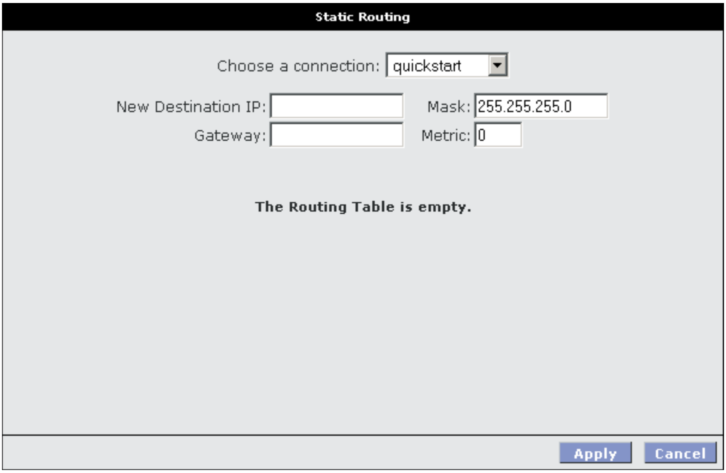
□ Enable IGMP Multicast

Select	Available Connections
○	quickstart

If you want to enable IGMP multicast, check **Enable IGMP Multicast**, select the WAN connection from the **Available Connections** list and click **Apply**.

4.4.18 Static Routing

The Gateway allows you to manually program the router's routing table. Up to 16 routes can be added.



Static Routing

Choose a connection: quickstart

New Destination IP:

Mask: 255.255.255.0

Gateway:

Metric: 0

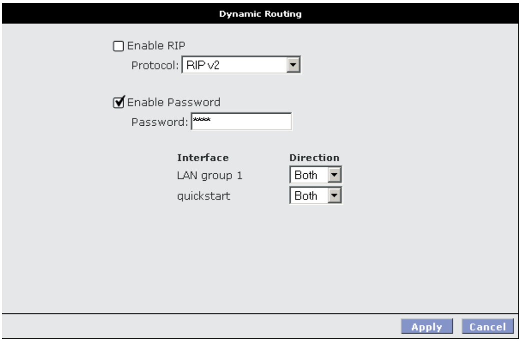
The Routing Table is empty.

For setting up static routing, please select a connection from the list, fill the **New Destination IP**, **Netmask**, **Gateway IP** and **Metric**. After that, click on **Apply**.

If you want to delete an existing static route, check the **Delete** checkbox next to the route information and click on **Apply**.

4.4.19 Dynamic Routing

Dynamic Routing uses RIP (Routing Information Protocol) for exchanging routing information with other routers in the network. It is supported across both WAN and LAN interfaces. When RIP (Routing Information Protocol) is enabled the router builds its own routing tables utilizing request and response packets. A request packet tells the router to build a list of its routing table contents with the network/host IP to which the table belongs, Netmask for the network and RIP host. After obtaining this information, the router will send a response to the machine that sent the original request. RIP will also update the main routing table.



□ Enable RIP
Protocol: RIP v2

☑ Enable Password
Password: ****

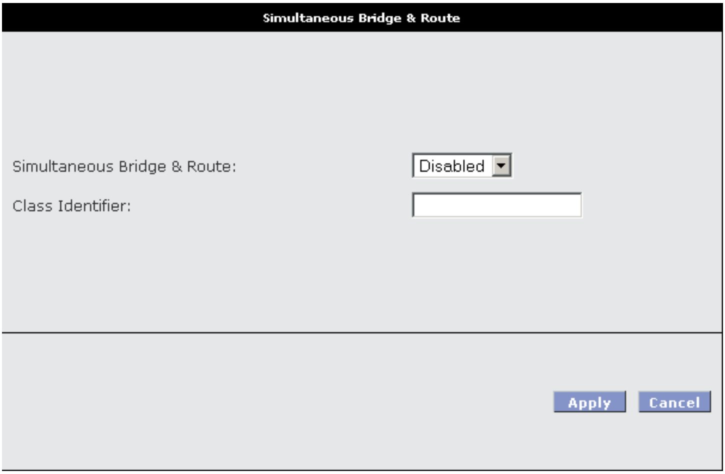
Interface	Direction
LAN group 1	Both
quickstart	Both

In the table below you can see the description of this page.

Field	Description
Enable RIP	Enable/Disable RIP
Protocol	The following three RIP versions are available: •RIP v1 •RIP v2 •RIP v1 compatible.
Enable Password	The 16 character long plain text password.
Password	Netmask of the source IP on your LAN side.
Direction	Normally when RIP is enabled on a router it dynamically learns routes on all it's configured interfaces. This parameter allows the user to select the interfaces on which RIP is expected to learn and distribute routing information. This feature allows the user to control how and which routes get distributed through the network e.g. prevent routes to the private LAN networks from being sent over to the WAN side router. The following four direction options are available: • Both: Receive updates on the interface and also send it's routing table to other routers connected to that interface. • In: Receive routing updates from other routers connected to that interface but NOT send routing updates on that interface. • Out: Send routing updates but not receive updates on this interface from the other routers connected to that interface • None: Ignores this interface and not send or receive routing updates through this interface.

4.4.20 Simultaneous Bridge & Route

Enabling this option will allow that special devices like set top boxes (STB) will get a public address from the ISP and send/receive packets directly from the ISP without being routed.



Simultaneous Bridge & Route

Simultaneous Bridge & Route: Disabled

Class Identifier:

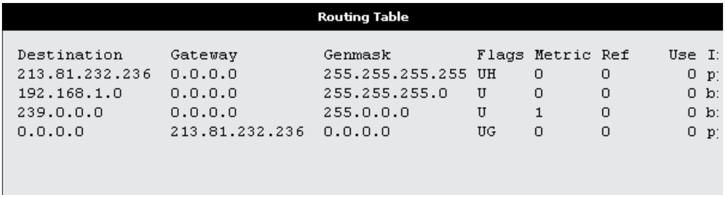
Every device that connects to the modem has its own class identifier. A set top box also has its own identifier. Whenever the set top box connects to the Gateway, it will send a DHCP discovery. The Gateway will check the DHCP option 60 in the packet. If the option 60 identifier matches the identifier stored in the Gateway, the Gateway will remember the MAC address of the STB. All incoming LAN traffic with the source MAC address matching the MAC address stored in the Gateway will be directly sent to the ISP. All incoming traffic from the ISP going to the destination MAC address stored in the Gateway will be sent directly to STB without any routing.

Only one PVC and one MAC address is supported at the moment.

Note: You must not enter your PC's identifier (MSFT 5.0) into the class identifier field. If you do so, your PC will not be able to get access to any webpage anymore.

4.4.21 Routing Table

This screen show the current routing table of the *ADSL2+ Wireless Gateway G*.



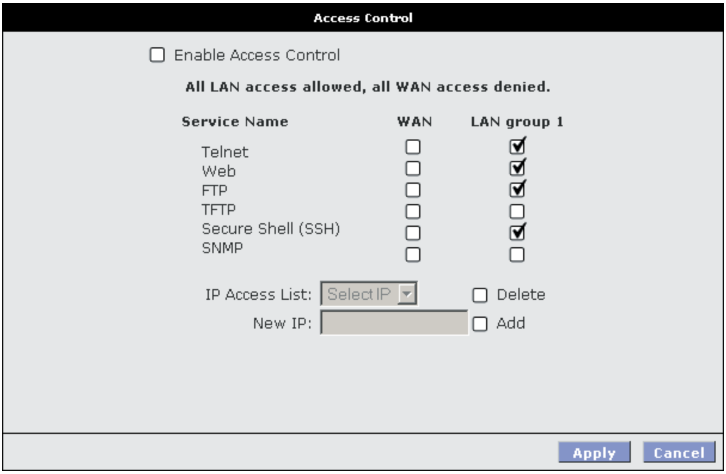
Routing Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use I:
213.81.232.236  0.0.0.0         255.255.255.255 UH    0      0        0 p:
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 b:
239.0.0.0       0.0.0.0         255.0.0.0       U     1      0        0 b:
0.0.0.0         213.81.232.236  0.0.0.0         UG    0      0        0 p:
```

4.4.22 Access Control

Access control allows you to open the access from the Internet (WAN) or LAN to the following management ports of the Gateway:

- Telnet
- Web
- FTP
- TFTP
- Secure Shell (SSH)
- SNMP



Access Control

□ Enable Access Control

All LAN access allowed, all WAN access denied.

Service Name	WAN	LAN group 1
Telnet	□	☑
Web	□	☑
FTP	□	☑
TFTP	□	□
Secure Shell (SSH)	□	☑
SNMP	□	□

IP Access List: Select IP □ Delete

New IP: □ Add

As you can see from the picture, the Access Control is disabled by default, remote management from the WAN side IP addresses is denied, most services from the LAN side IP addresses are enabled.

Access Control, when enabled, supports up to 16 IP addresses with controlled (allow/deny) WAN and/or LAN access.

Note: If no IP addresses are specified within the IP Access List, the access control list will be disabled until the first IP address is added.

Use the following procedure to enable Access Control and add an WAN IP address and a LAN IP address to the access control list.

1. Check **Enable Access Control** to enable the feature. This will enable the IP Access List field.

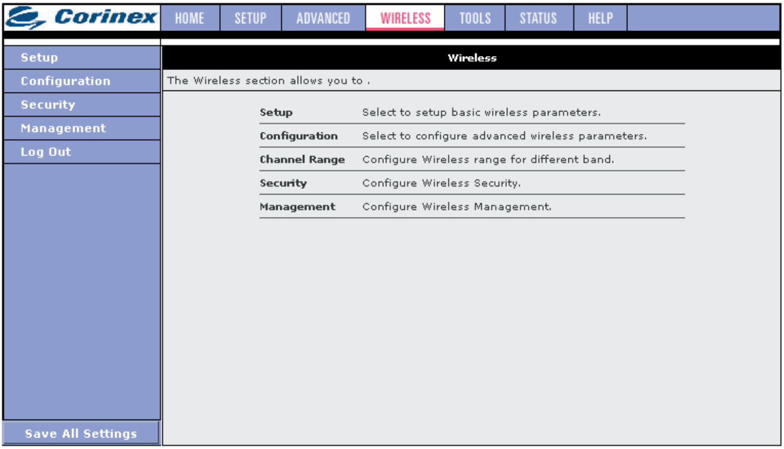
2. You can select an IP from the IP Access List, or enter a new IP and check **Add**.

3. Change the LAN and/or WAN configurations of the IP address.

4. Click **Apply**.

4.5 Wireless tab

In this tab you can configure the settings for the wireless access point in your Gateway. By clicking on the **Wireless** tab the following page opens.



Wireless

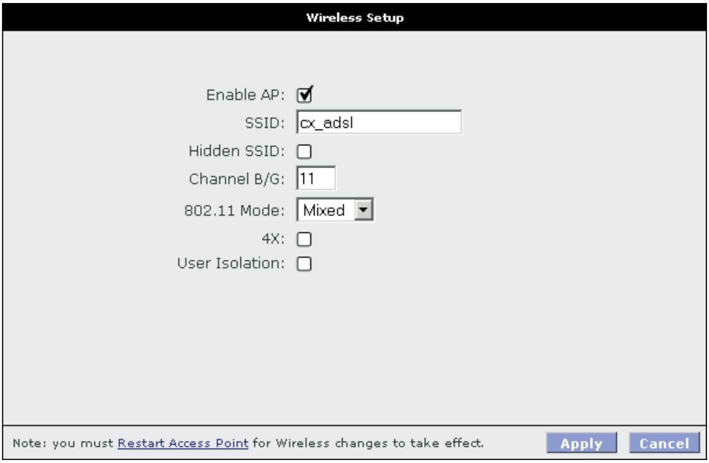
The Wireless section allows you to .

Setup	Select to setup basic wireless parameters.
Configuration	Select to configure advanced wireless parameters.
Channel Range	Configure Wireless range for different band.
Security	Configure Wireless Security.
Management	Configure Wireless Management.

In the left menu there are the following sections.

4.5.1 Setup

In the Setup section you can configure basic wireless parameters. Click on **Setup** in the left menu, the following screen will appear:


Wireless Setup

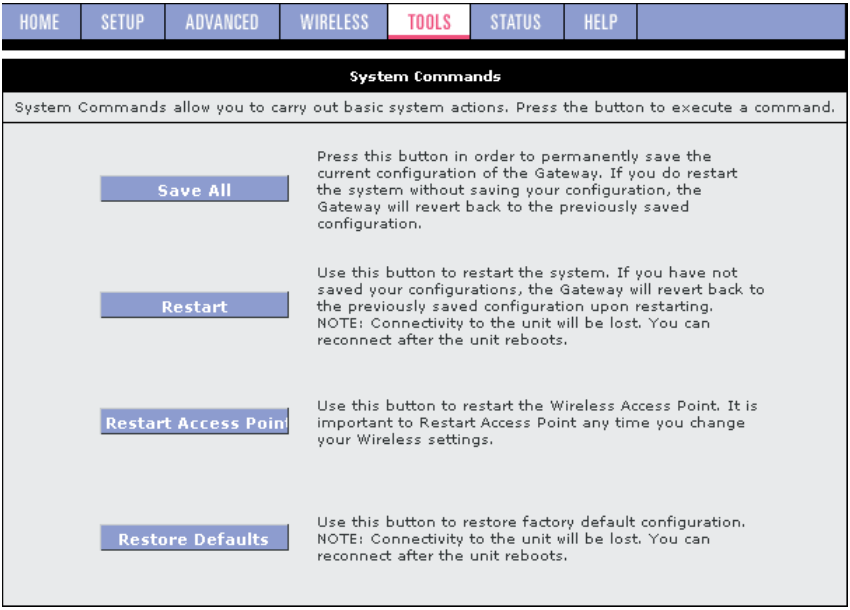
Enable AP: ☑
SSID: cx_adsl
Hidden SSID: □
Channel B/G: 11
802.11 Mode: Mixed
4X: □
User Isolation: □

Note: you must Restart Access Point for Wireless changes to take effect.

The table below describes the options in this page:

Option	Description
Enable AP	The wireless setup allows the user to enable or disable the AP (access point). Disabling of AP will prevent the Gateway from emitting or receiving any wireless signal.
SSID	Here you can enter your SSID which is an identification string for your wireless access point
Hidden SSID	If this field is checked, the access point will not send the SSID to other wireless enabled devices in the range.
Channel B/G	You can select the channel for transmission of the wireless access point. Please note that not all channels are allowed in each country. Refer to the following regulation information (IEEE STD 802.11b-1999/Cor 1-2001): - Europe: channels 1-13 - USA/Canada : channels 1-11 - Japan: channels 1-14 - Spain: channels 10 &11
802.11 Mode	You can select the mode so that only selected wireless devices can connect to your access point: - **Mixed**: both 802.11b and 802.11g devices can connect - **B only** : only 802.11b devices can connect - **B+**: both devices with 802.11b and enhanced 802.11b+ (22 Mbps) can connect - **G only** : only 802.11g devices can connect
4x	If this is checked, the access point switches to the enhanced 44 Mbps throughput rate. This mode is backwards compatible with 802.11b

After the configuration, click **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands** section in the **Tools** tab as shown below and click on **Restart Access Point**.



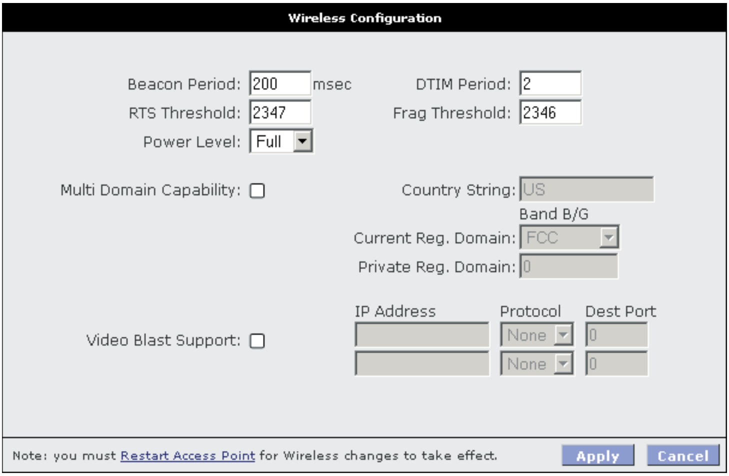
System Commands

System Commands allow you to carry out basic system actions. Press the button to execute a command.

Save All	Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart	Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restart Access Point	Use this button to restart the Wireless Access Point. It is important to Restart Access Point any time you change your Wireless settings.
Restore Defaults	Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

4.5.2 Configuration

In this section you can configure advanced wireless parameters. After clicking on **Configuration** in the left menu, the following screen will appear:



Wireless Configuration

Beacon Period: 200 msec
DTIM Period: 2
RTS Threshold: 2347
Frag Threshold: 2346
Power Level: Full
Multi Domain Capability: □
Country String: US
Band B/G
Current Reg. Domain: FCC
Private Reg. Domain: 0
Video Blast Support: □

IP Address	Protocol	Dest Port
	None	0
	None	0

Note: you must Restart Access Point for Wireless changes to take effect.

The table below describes the available settings:

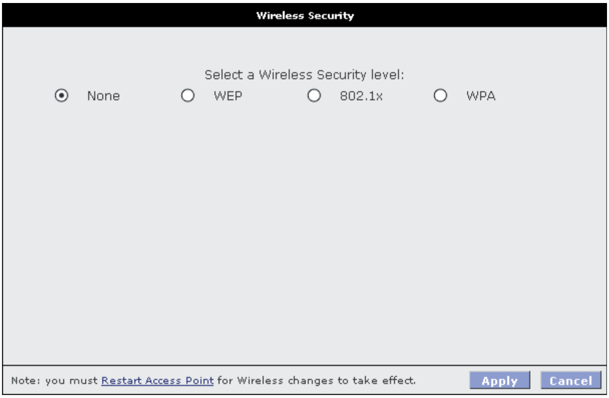
Field	Value
Beacon Period	Beacon Period is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon period to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The default value is 200.
DTIM Period	DTIM stands for Delivery Traffic Indication Message. A DTIM is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast message for associated clients, it sends the next DTIM with a DTIM Period value. Access point clients hear and awaken to receive the broadcast and multicast messages. The default DTIM period is '2'.
RTS Threshold	The 802.11 standard includes the RTS/CTS (Request to Send/Clear to Send) function to control access of the wireless stations to the wireless medium. If two wireless stations are transmitting packets to the access point at the same time, the access point will not be able to handle both, and one of the stations will have to repeat the transmission. If the RTS/CTS function is enabled, the station will initiate a handshake with the destination device (access point). After the access point finishes all pending operations, it confirms that the station can send the packet. This improves performance by avoiding repeat transmissions of the same data. The threshold value is the maximum size of a packet which can be sent without activating the RTS/CTS handshake. Sending a packet with a size larger than the threshold value will activate the RTS/CTS handshake before transmission can begin. By default, the RTS/CTS function is disabled– the threshold is set to 2347 bytes.

Field	Value
Frag Threshold	In case of interference in the wireless channel, or weak coverage, the *Corinex ADSL2+ Wireless Gateway G* can fragment frames to optimize performance. It will divide the frames into smaller pieces and send them separately to the recipient. Only data packets are fragmented, the broadcast and multicast packets are transmitted unchanged. The threshold value means the maximum size of an unfragmented packet. Any frame larger than that threshold will be fragmented. If there are no packet losses in the wireless media, the value should be unchanged. If you experience collisions, try to lower the threshold to approx. 1000 bytes. If the network performs well at this setting, you can try higher values until you find the optimal performance. The default value of the threshold is 2346 bytes.
Power Level	You can choose the percentage of maximum power output to meet your requirement. The default is Full.

After the configuration, click on **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands section** in the **Tools** tab as shown below and click on **Restart Access Point**.

4.5.3 Security

In this section you can configure the security settings for the wireless access point. After clicking on **Security** in the left menu, the following screen will appear.



Wireless Security

Select a Wireless Security level:

● None ○ WEP ○ 802.1x ○ WPA

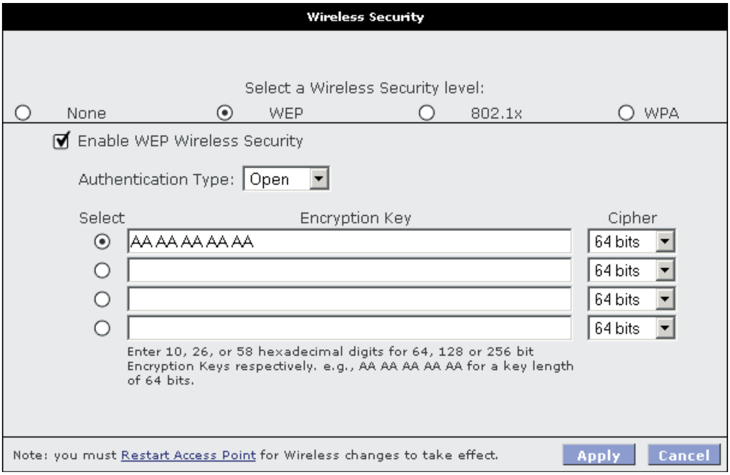
Note: you must Restart Access Point for Wireless changes to take effect.

In the default settings, wireless security is disabled and anyone can connect to your access point. This setting is not recommended if you want to maintain a secure wireless network, prevent 3rd parties from using your internet connection and prevent any attacks into your local network.

You can select between WEP, 802.1x and WPA security.

WEP

After clicking on **WEP**, the following page opens.



Wireless Security

Select a Wireless Security level:

○ None ● WEP ○ 802.1x ○ WPA

☑ Enable WEP Wireless Security

Authentication Type: Open

Select	Encryption Key	Cipher
●	AA AA AA AA AA	64 bits
○		64 bits
○		64 bits
○		64 bits

Enter 10, 26, or 58 hexadecimal digits for 64, 128 or 256 bit Encryption Keys respectively. e.g., AA AA AA AA AA for a key length of 64 bits.

Note: you must Restart Access Point for Wireless changes to take effect.

You can enable or disable WEP security by selecting or unselecting the **Enable WEP Wireless Security** checkbox.

After enabling the WEP security, select the **Authentication Mode**. The respective settings are explained in the table below.

Authentication Mode	Description
Open	The simplest authentication method. After the wireless client sends out a request , the access point will authenticate it.
Shared	This method uses a WEP-encrypted password for authentication. The client is authenticated by the access point only if the passwords match.
Both	Open or Shared will be selected automatically.

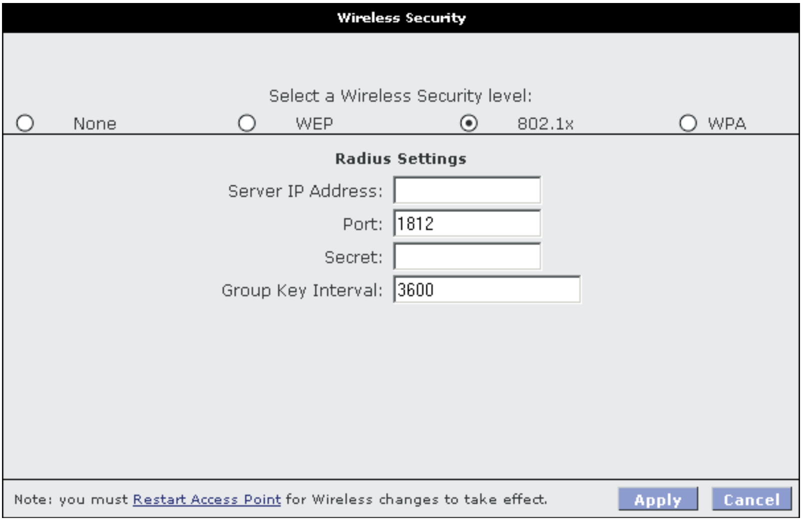
The communication between the access point and the wireless clients can be encrypted with 64-bit, 128-bit or 256-bit strong WEP encryption. Select the active key used for encryption from the 4 keys available, configure the length selecting a value from the **Cipher** field and enter the key in hexadecimal (0-9, A-F) format. The following table shows the required lengths of the WEP keys, depending on the **Cipher** setting.

Cipher	Key Length
64 bits	10
128 bits	26
256 bits	58

After the configuration, click **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands** section in the **Tools** tab as shown below and click on **Restart Access Point**.

802.1x

This method uses a Radius server for authentication. After clicking on **802.1x** the following screen appears.



Wireless Security

Select a Wireless Security level:

○ None ○ WEP ● 802.1x ○ WPA

Radius Settings

Server IP Address:

Port: 1812

Secret:

Group Key Interval: 3600

Note: you must Restart Access Point for Wireless changes to take effect.

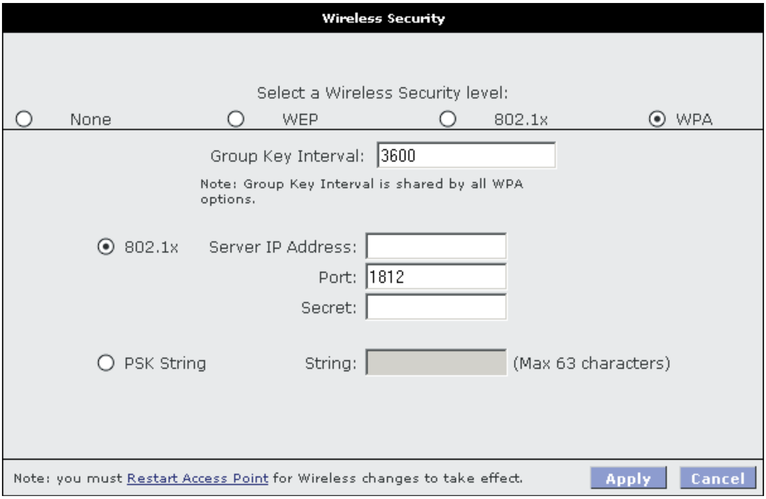
Please enter the IP Address of the Radius Server, specify the port (default is 1812), enter the Radius secret. The Group Key Interval is the rate that the RADIUS server sends a new Group Key out to all clients.

After the configuration, click **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands section** in the **Tools** tab as shown below and click on **Restart Access Point**.

WPA

WPA uses a combination of Open System and 802.1x authentication. First the wireless client authenticates with the access point, then performs user-level authentication with 802.1x.

After clicking on **WPA**, the following page opens.



Wireless Security

Select a Wireless Security level:

○ None ○ WEP ○ 802.1x ● WPA

Group Key Interval: 3600

Note: Group Key Interval is shared by all WPA options.

● 802.1x Server IP Address:

Port: 1812

Secret:

○ PSK String String: (Max 63 characters)

Note: you must Restart Access Point for Wireless changes to take effect.

The **Group Key Interval** is the rate that the RADIUS server sends a new Group Key out to all clients. By default it is set to 3600 seconds.

You can select between WPA and WPA PSK by selecting **802.1x** or **PSK String** in this page. The following table described both modes.

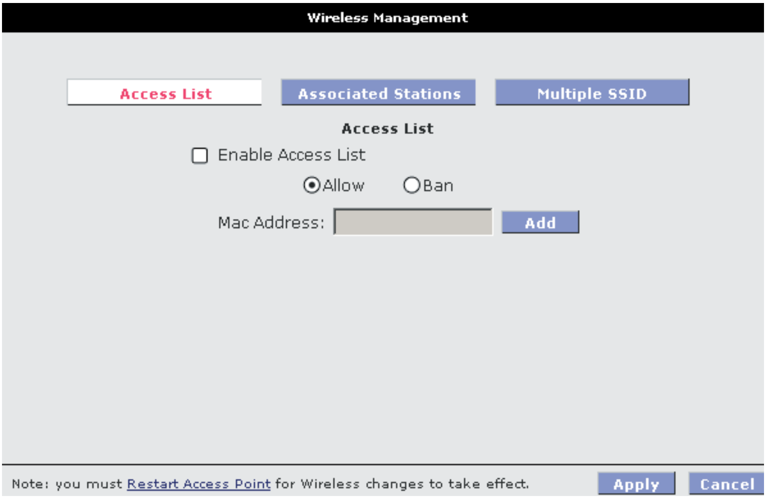
WPA Mode	Description
WPA	A Radius server is used for authentication. Please enter the IP Address of the Radius server, its port (1812 by default) and the secret.
WPA PSK	This mode doesn't require 802.1x authentication. The authentication in this mode is based on shared secrets, stored both on the access point and on the wireless client. Please enter the shared secret in the **String** field. The shared secret can be up to 63 characters long.

After the configuration, click **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands** section in the **Tools** tab as shown below and click on **Restart Access Point**.

4.5.4 Management

The Wireless Management allows you to set up access rights for wireless clients. You can set up a list of allowed or banned wireless clients, view the associated clients, or set up multiple SSID for your access point.

After clicking on **Management** in the left menu, the following page will appear.



Wireless Management

Access List

□ Enable Access List

● Allow ○ Ban

Mac Address:

Note: you must Restart Access Point for Wireless changes to take effect.

Access List

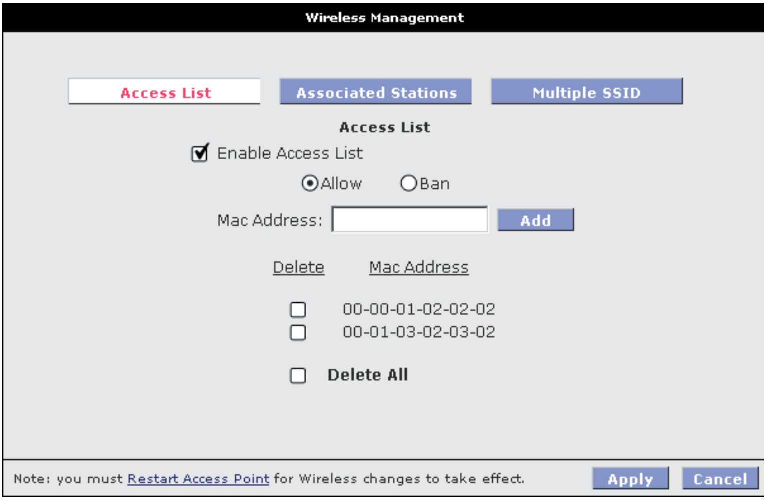
The **Access List** functions allows you to **Allow** or **Ban** any wireless client from accessing the Gateway.

After enabling the Access List function by checking the **Enable Access List** checkbox, select the requested functionality, which is described in the table below.

Method	Description
Allow	Wireless clients specified in the list will be allowed to connect to the Gateway.
Ban	Wireless clients specified in the list will not be allowed to connect to the Gateway.

After that, input the MAC adresses of the wireless clients in the format xx-xx-xx-xx-xx-xx and click **Add**.

After you have entered the MAC addresses, you will see a screen similar to the one below.



Access List

☑ Enable Access List

● Allow ○ Ban

Mac Address:

Delete	Mac Address
□	00-00-01-02-02-02
□	00-01-03-02-03-02

□ Delete All

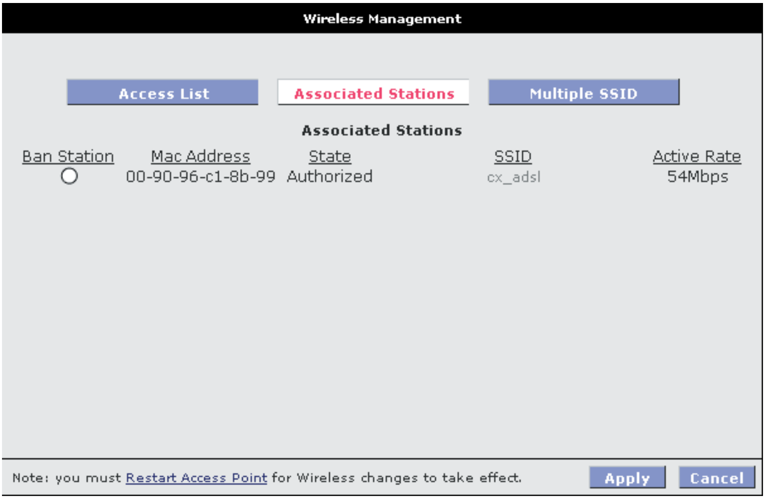
Note: you must Restart Access Point for Wireless changes to take effect.

You can delete the MAC addresses from the list by checking the **Delete** checkbox next to the MAC address and clicking **Apply**. If you want to delete all the MAC addresses from the list, select **Delete All** and click **Apply**.

After the configuration, click **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands** section in the **Tools** tab as shown below and click on **Restart Access Point**.

Associated Stations

After clicking on **Associated Stations**, the following screen will appear.

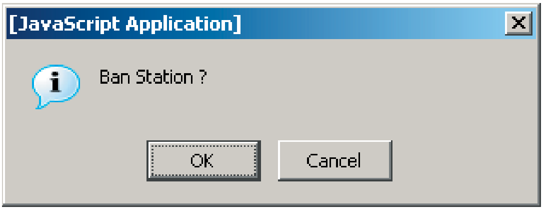


Associated Stations

Ban Station	Mac Address	State	SSID	Active Rate
○	00-90-96-c1-8b-99	Authorized	cx_adsl	54Mbps

Note: you must Restart Access Point for Wireless changes to take effect.

Here you can see all associated wireless stations, which are connected to your Gateway. If you want to prevent any client from connecting to the Gateway, click on **Ban Station**. The following window will appear.



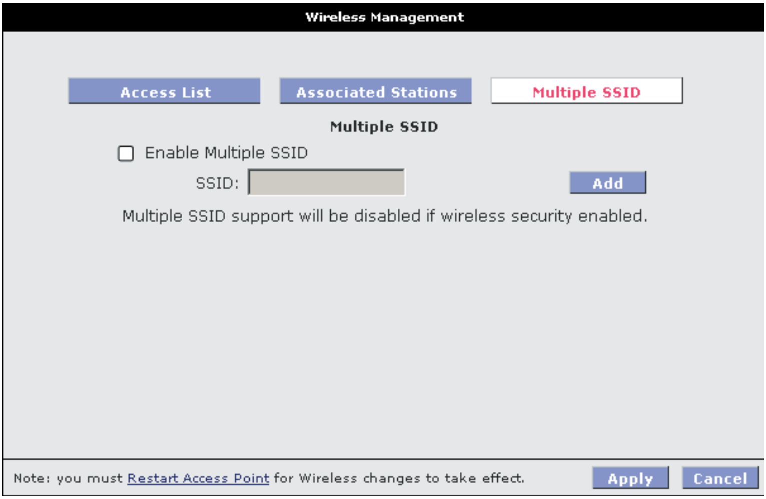
Ban Station ?

Click **OK** to ban the wireless client.

After the configuration, click **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands** section in the **Tools** tab as shown below and click on **Restart Access Point**.

Multiple SSID

The Gateway supports multiple SSID, all of them can be set in the following screen.



Wireless Management

Multiple SSID

□ Enable Multiple SSID

SSID:

Multiple SSID support will be disabled if wireless security enabled.

Note: you must Restart Access Point for Wireless changes to take effect.

Note: Multiple SSID support will be disabled if wireless security is enabled.

You can enter a new SSID into the **SSID**: field and click **Add**.

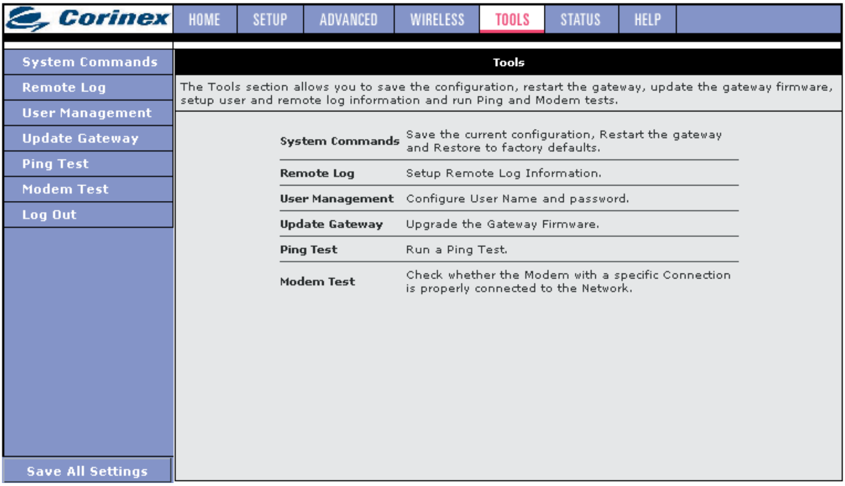
If you want to delete any of the assigned SSID strings, you can click the radio button **Delete** in front of the displayed SSID.

After the configuration, click **Apply**. To enable the new settings you will have to restart the access point. Please go to the **System Commands** section in the **Tools** tab as shown below and click on **Restart Access Point**.

4.6 Tools Tab

The Tools section allows you to save the configuration, restart the gateway, update the gateway firmware, setup user and remote log information and run Ping and Modem tests.

After clicking on the **Tools** tab, the following screen will appear.



Tools

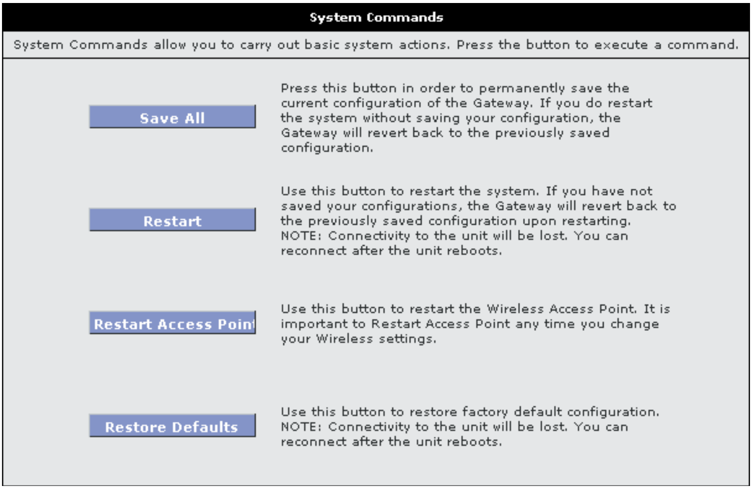
The Tools section allows you to save the configuration, restart the gateway, update the gateway firmware, setup user and remote log information and run Ping and Modem tests.

System Commands	Save the current configuration, Restart the gateway and Restore to factory defaults.
Remote Log	Setup Remote Log Information.
User Management	Configure User Name and password.
Update Gateway	Upgrade the Gateway Firmware.
Ping Test	Run a Ping Test.
Modem Test	Check whether the Modem with a specific Connection is properly connected to the Network.

Below you can find the description for the commands in the left menu.

4.6.1 System Commands

After clicking on **System Commands**, the following page appears.



System Commands

System Commands allow you to carry out basic system actions. Press the button to execute a command.

Save All	Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart	Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restart Access Point	Use this button to restart the Wireless Access Point. It is important to Restart Access Point any time you change your Wireless settings.
Restore Defaults	Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Press one of the buttons to execute a system command. The commands are described in the following table.

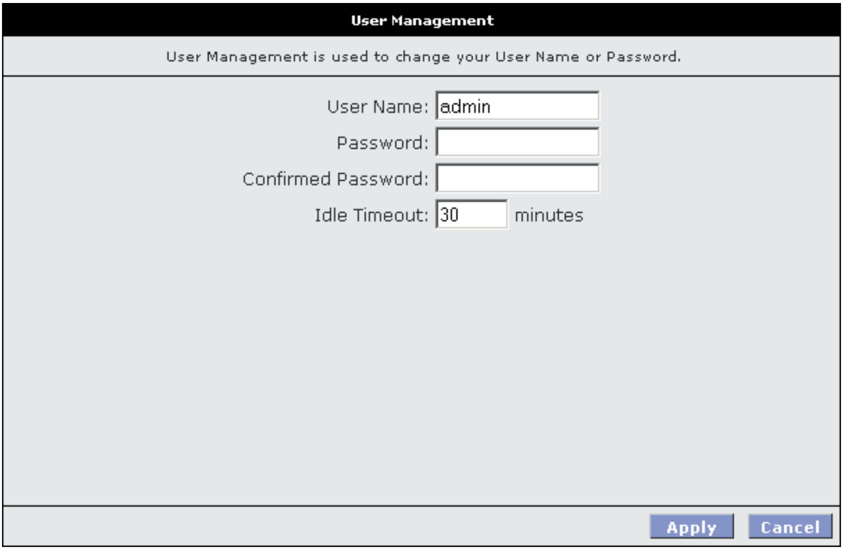
Field	Description
Save All	Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart	Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. **NOTE**: Connectivity to the unit will be lost. You can re-connect after the unit reboots.
Restart Access Point	Use this button to restart the Wireless Access Point. It is important to Restart Access Point any time you change your Wireless settings.
Restore Defaults	Use this button to restore factory default configuration. **NOTE**: Connectivity to the unit will be lost. You can re-connect after the unit reboots

4.6.2 Remote Log

The Gateway is able to capture everything that happens during operation using the Remote Log (or Syslog) function. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors - also known as syslog servers.

4.6.3 User Management

In this section you can change the username and password which are used for securing this configuration web interface.



User Management

User Management is used to change your User Name or Password.

User Name: admin

Password:

Confirmed Password:

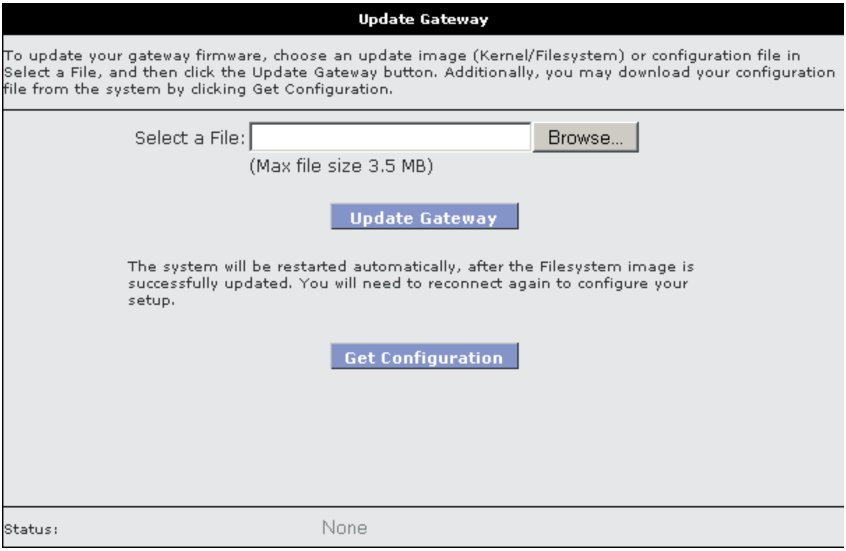
Idle Timeout: 30 minutes

To change the username and password, enter the **User Name**, enter the **Password**, confirm it again in **Confirmed Password** and set the **Idle Timeout**. The idle timeout is the time of inactivity, after which the user will be logged out from the configuration web interface. The default setting is 30 minutes.

After the change, click **Apply**. Don't forget to permanently save the configuration by clicking **Save All Settings** in the left menu.

4.6.4 Update Gateway

As we are constantly innovating our products, it may happen that there is a newer version of the firmware for the Gateway released. Usually it can be downloaded from our website www.corinex.com. In this section, you can update your Gateway to the latest firmware version.



Update Gateway

To update your gateway firmware, choose an update image (Kernel/Filesystem) or configuration file in Select a File, and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.

Select a File: [ ] Browse...

(Max file size 3.5 MB)

The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.

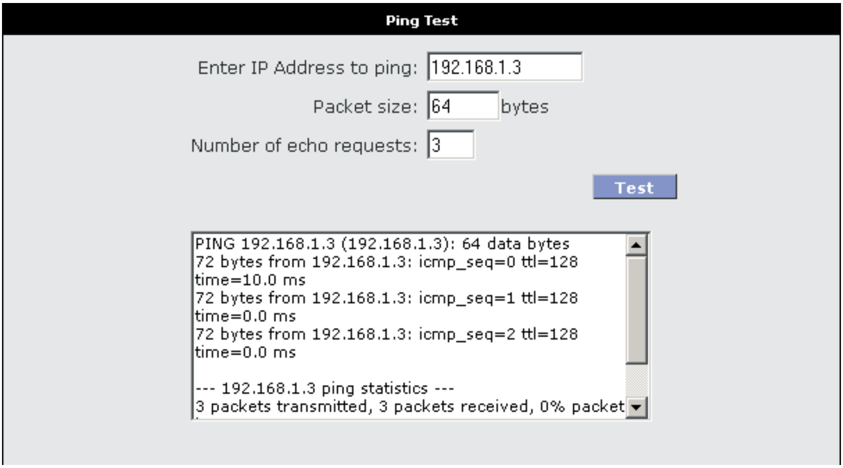
Status: None

To update your gateway firmware, choose an update image (Kernel/Filesystem) or configuration file in **Select a File**, and then click the **Update Gateway** button. Additionally, you may download your configuration file from the system by clicking **Get Configuration**.

The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.

4.6.5 Ping Test

Once you have your Gateway configured, it is a good idea to make sure you can ping the network. You can get to the Ping Test page by clicking on **Ping Test** in the left menu.



Enter IP Address to ping: 192.168.1.3

Packet size: 64 bytes

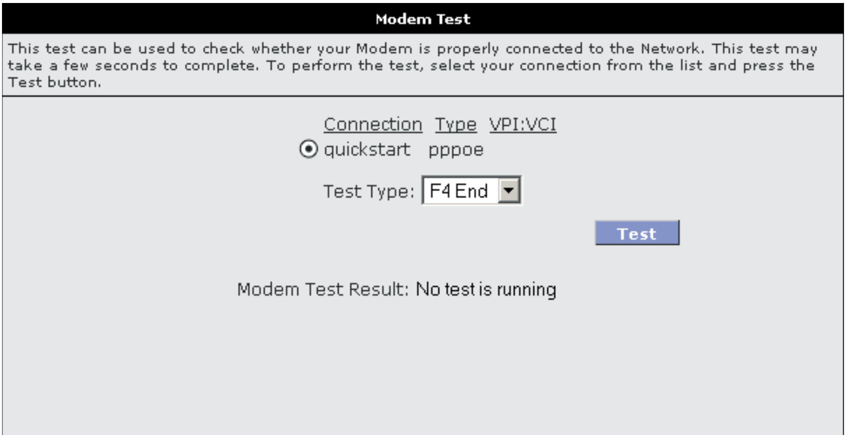
Number of echo requests: 3

```
PING 192.168.1.3 (192.168.1.3): 64 data bytes
72 bytes from 192.168.1.3: icmp_seq=0 ttl=128
time=10.0 ms
72 bytes from 192.168.1.3: icmp_seq=1 ttl=128
time=0.0 ms
72 bytes from 192.168.1.3: icmp_seq=2 ttl=128
time=0.0 ms

--- 192.168.1.3 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet
```

Type the target address that you want to ping. If you have your PC connected to the Gateway via the default DHCP configuration, you should be able to Ping the network address 192.168.1.1. If your ISP has provided their server address you can try to ping the address. If the pings for both the WAN and the LAN side complete, and you have the proper protocols configured, you should be able to surf the Internet.

4.6.6 Modem Test

This test can be used to check whether the modem is properly connected to the network.



This test can be used to check whether your Modem is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button.

Connection	Type	VPI:VCI
● quickstart	pppoe	

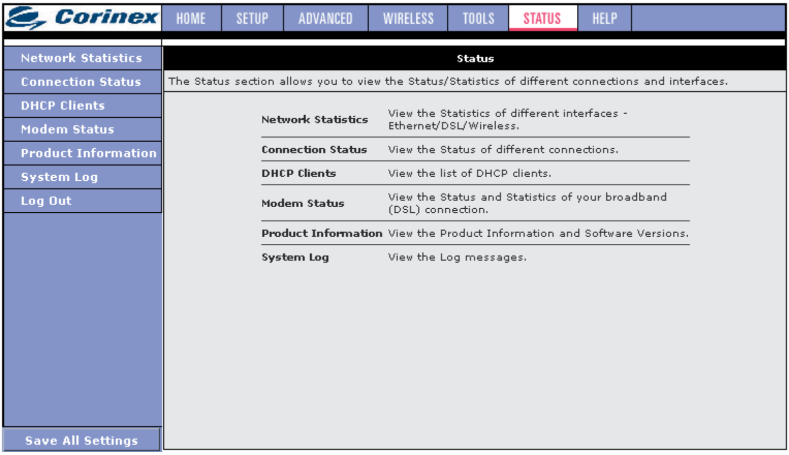
Test Type: F4 End

Modem Test Result: No test is running

To perform the test, select your connection from the list and the test type and press the **Test** button. After a while the result of the test will be displayed.

4.7 Status Tab

The Status section allows you to view the Status/Statistics of different connections and interfaces. It also shows information about the modem, firmware version and the system log:



Status

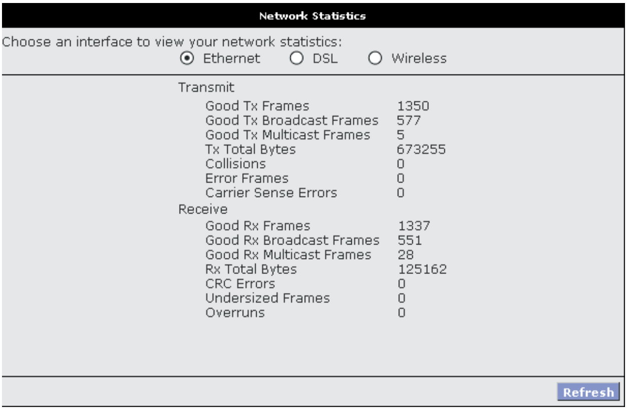
The Status section allows you to view the Status/Statistics of different connections and interfaces.

Network Statistics	View the Statistics of different interfaces - Ethernet/DSL/Wireless.
Connection Status	View the Status of different connections.
DHCP Clients	View the list of DHCP clients.
Modem Status	View the Status and Statistics of your broadband (DSL) connection.
Product Information	View the Product Information and Software Versions.
System Log	View the Log messages.

Select one of the available sections from the left menu to view the required information.

4.7.1 Network Statistics

The network statistics page shows the traffic statistics for every network interface of your Gateway. You can click on the interface name (Ethernet, DSL or Wireless) to view the statistics.



Network Statistics

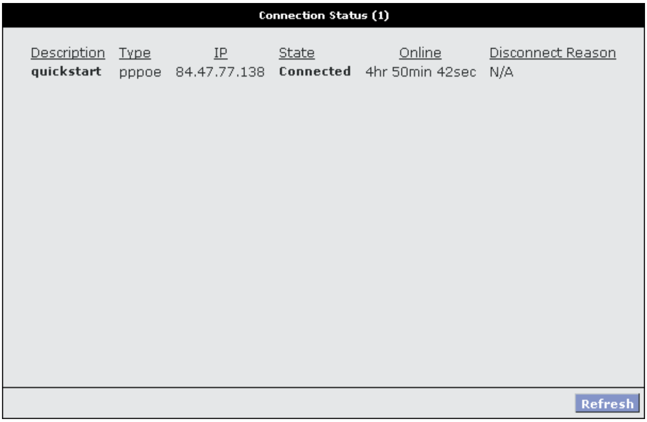
Choose an interface to view your network statistics:
● Ethernet ○ DSL ○ Wireless

```
Transmit
    Good Tx Frames                1350
    Good Tx Broadcast Frames      577
    Good Tx Multicast Frames      5
    Tx Total Bytes                673255
    Collisions                    0
    Error Frames                  0
    Carrier Sense Errors          0
Receive
    Good Rx Frames                1337
    Good Rx Broadcast Frames      551
    Good Rx Multicast Frames      28
    Rx Total Bytes                125162
    CRC Errors                    0
    Undersized Frames             0
    Overruns                      0
```

By clicking the **refresh** button the page will be reloaded with the latest statistics.

4.7.2 Connection Status

Connection Status will display all the relevant information regarding your Internet Connection, it will display the type of protocol used, the WAN IP address, the connection status, and the duration of the connection. In case the connection is disconnected, the reason for this will be displayed.



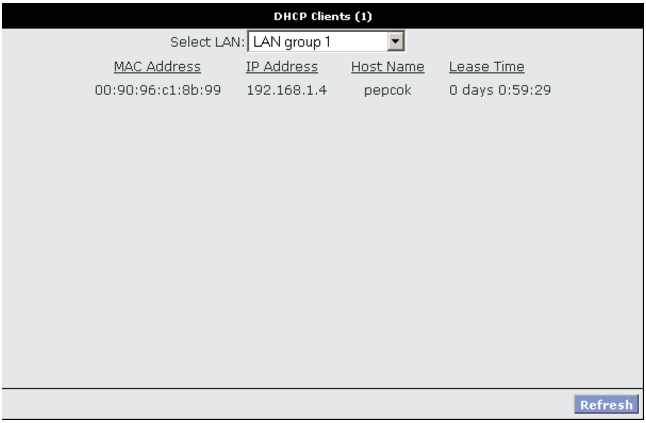
Connection Status (1)

Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	84.47.77.138	**Connected**	4hr 50min 42sec	N/A

By clicking the **refresh** button the page will be reloaded with the latest information.

4.7.3 DHCP Clients

This screen shows the list of DHCP clients for each configured LAN group which has a running DHCP server.



DHCP Clients (1)

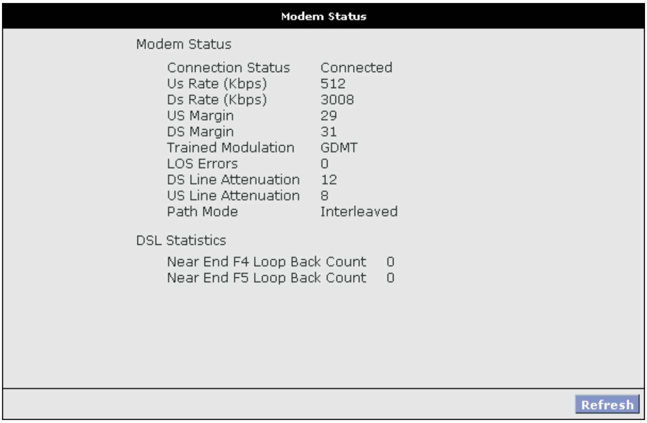
Select LAN: LAN group 1

MAC Address	IP Address	Host Name	Lease Time
00:90:96:c1:8b:99	192.168.1.4	pepcok	0 days 0:59:29

You can select a LAN group from the list to view the list of associated DHCP clients. By clicking the **refresh** button the page will be reloaded with the latest DHCP client table.

4.7.4 Modem Status

This screen will display the Modem status and DSL statistics. If the modem is disconnected the reason for this will be displayed.

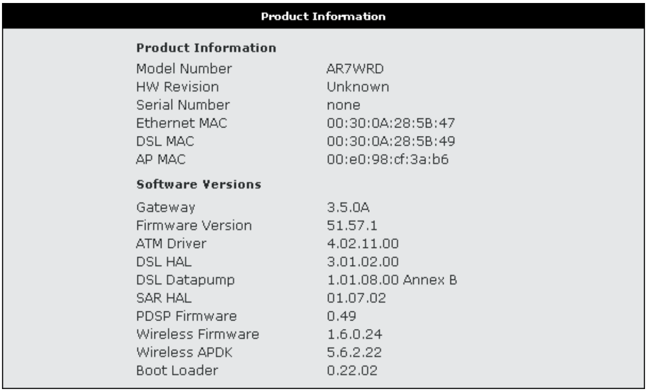


```
Modem Status

Modem Status
    Connection Status      Connected
    Us Rate (Kbps)         512
    Ds Rate (Kbps)         3008
    US Margin              29
    DS Margin              31
    Trained Modulation     GDMT
    LOS Errors             0
    DS Line Attenuation    12
    US Line Attenuation    8
    Path Mode              Interleaved

DSL Statistics
    Near End F4 Loop Back Count    0
    Near End F5 Loop Back Count    0
```

By clicking the **refresh** button the page will be reloaded with the latest statistics.

4.7.5 Product Information

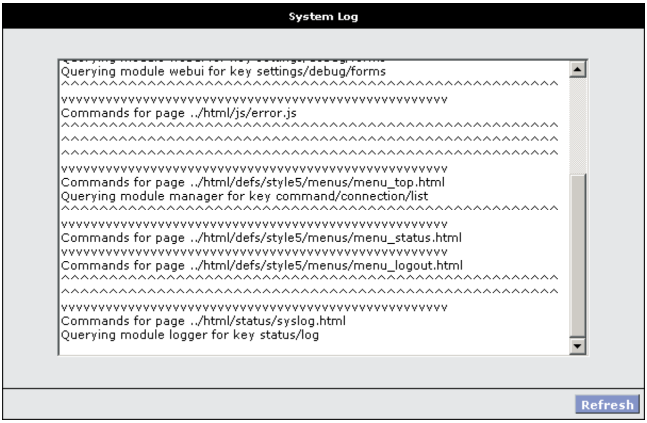
This screen will show a summary of all the product information and software version that comes bundled with the Gateway.



```
Product Information

Product Information
Model Number           AR7WRD
HW Revision            Unknown
Serial Number          none
Ethernet MAC           00:30:0A:28:5B:47
DSL MAC                00:30:0A:28:5B:49
AP MAC                 00:e0:98:cf:3a:b6

Software Versions
Gateway                3.5.0A
Firmware Version       51.57.1
ATM Driver             4.02.11.00
DSL HAL                3.01.02.00
DSL Datapump           1.01.08.00 Annex B
SAR HAL                01.07.02
PDSP Firmware          0.49
Wireless Firmware      1.6.0.24
Wireless APDK          5.6.2.22
Boot Loader            0.22.02
```

4.7.4 System Log

Here you can see the Gateway's system log.

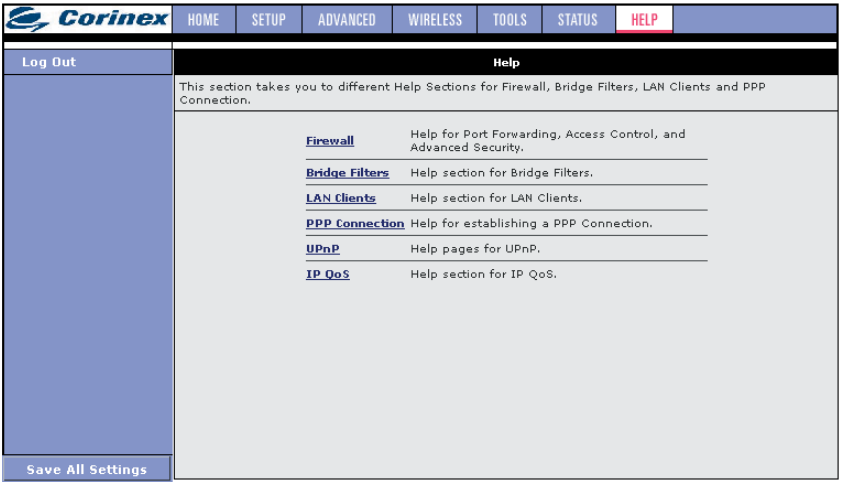


```
Querying module webui for key settings/debug/forms
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
Commands for page ../html/js/error.js
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
Commands for page ../html/defs/style5/menus/menu_top.html
Querying module manager for key command/connection/list
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
Commands for page ../html/defs/style5/menus/menu_status.html
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
Commands for page ../html/defs/style5/menus/menu_logout.html
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
Commands for page ../html/status/syslog.html
Querying module logger for key status/log
```

Depending on the log level chosen in the **Tools -> Remote Log**, the appropriate information will be displayed. By clicking the **refresh** button the page will be reloaded with the latest information.

4.8 Help Tab

This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients and PPP Connection.



Help

This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients and PPP Connection.

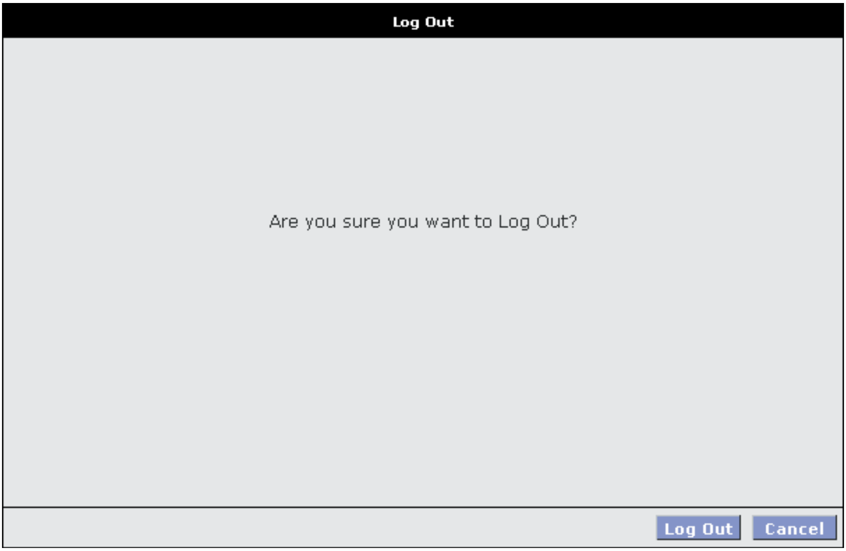
Firewall	Help for Port Forwarding, Access Control, and Advanced Security.
Bridge Filters	Help section for Bridge Filters.
LAN Clients	Help section for LAN Clients.
PPP Connection	Help for establishing a PPP Connection.
UPnP	Help pages for UPnP.
IP QoS	Help section for IP QoS.

You can click on one of the links **Firewall, Bridge Filters, LAN Clients, PPP Connection, UPnP** or **IP QoS** to display additional information about the topic.

Note: In every configuration section, there are two common buttons in the left menu which allow you to save the settings into the Gateway's memory or log out from the configuration interface.

Log out

If you finished with configuration of the Gateway and saved all settings, you can log out. By clicking **Log Out**.



Are you sure you want to Log Out?

If you want to log out of the Gateway's web interface, click on **Log Out**. You will be logged out and the authentication screen appears.

Save Settings

If you changed any settings, you must save them so that they will appear when the Gateway boots up next time. Please click on **Save Settings**, the latest changes will be written into the flash memory. After that you can reset or power off your gateway without losing the changes in configuration.

Appendix A: Troubleshooting

A.1 Troubleshooting Guide

This section provides possible solutions to problems regarding the installation and operation of the *Corinex ADSL2+ Wireless Gateway G*. Read the description below to solve your problems. If you can not find an answer here, check the Corinex website at www.corinex.com.

Computer networking can sometimes be "tricky" when many components must work together to function properly for the ultimate network system. The problems are usually easy to fix with the right tools. The following tools, available on your computer, will get you started.

- Ping (from the command prompt)
- ipconfig (WinNT/2000/XP), winipcfg (Win9x/Me) (from the command prompt)

If it just doesn't work...

1. Check that the Power LED on the *Corinex ADSL2+ Wireless Gateway G* if it is on, if not:
   - Check the AC cord.
   - Make sure the AC outlet is working by plugging something else into it. If this works, try another outlet. If this fails as well, try 2. – 4.
2. Check the Ethernet cables:
   The *Corinex ADSL2+ Wireless Gateway G* has LEDs on the LAN part of the Ethernet side labeled **E1-E4**. If they are not on:
   - Check if the device at the other end of the Ethernet cable is switched on.
   - Try a different Ethernet cable.
3. Check that TCP/IP detects the *Corinex ADSL2+ Wireless Gateway G*:
   From the command prompt, run **ping** and type the computer name or IP address of the computer you are working on [ping your computer name]. This should return 4 good packets. Now try to ping another computer on the network. If a timeout occurs:
   - Go into the TCP/IP properties and check that the buttons for automatically obtaining IP addresses and gateway are checked. If not, make sure that both computers are on the same subnet.
   - Run **ipconfig/all** from the command prompt on all computers to verify that all computers have valid IP addresses on the same subnet.
   - The IP tables may be corrupted, reboot all computers and try again. If these tests work, you have basic connectivity and can use all network services. If this does not work, you may have a faulty device. Please contact your reseller or local distributor.

I have got all that, it still doesn't work...

- Make sure that your TCP/IP settings are set to automatically obtaining IP address and gateway address. If the DHCP server is not running on the network, than set the TCP/IP configuration manually as described in the *chapter 3.2*.
- Switch off all computers. This will ensure that the computer's IP address will be obtained from the Gateway.
- Now open the web browsers, if the "Not Found" page appears, try to check your LAN settings in the Internet Options of your web browser.

Wireless part…

The Wireless LED does not light up on the Gateway.

- When the Wireless port detects a WLAN connection, the Wireless LED will be blinking. Check the Wireless adapter on your computer to see if connection and adapter work properly.
  Check the Wireless configuration of the Wireless adapter on your computer.

I am getting interference between my other 2.4 GHz wireless devices and my wireless network.

You can take several steps:

- Change the channel of the other 2.4 GHz Wireless devices or the Access Point so that they can use different channels.
- Move wireless devices farther away from the Access Point space.

The Gateway is not functional.

1. Check that the power LED is green and than the network cables are installed correctly. Refer to the easy start guide for more details.

2. Check that the **ETH** and **Internet** LEDs are green.

3. Check that the **DSL** LED is green.

4. Check the settings on your PC. Again, refer to the easy start guide for more details.

5. Check the Gateway's settings.

6. From your PC, can you PING the Gateway? Assuming that the Gateway has DHCP enabled and your PC is on the same subnet as the gateway, you should be able to PING the gateway.

7. Can you PING the WAN IP? Your ISP should have provided the IP address of their server. If you can ping the Gateway and your protocols are configured correctly, you should be able to ping the ISPs network. If you cannot PING the ISPs network, make sure you are using the correct protocols with the correct VPI VCI values.

8. Make sure **NAT** is enabled for your connection. If NAT is disabled the Gateway will not route frames correctly (except in Bridge connection).

I can't connect to the Gateway.

1. Check that the **Power** LED is green and that the network cables are installed correctly; see the easy start guide for more details.

2. Make sure that your PC and the Gateway is on the same network segment. The Gateway's default IP address is 192.168.1.1. If you are running a Windows based PC, you can open a DOS window and type **IPCONFIG**; make sure that the network adapter that is connected to the gateway is within the same 192.168.1.x subnet.

3. Also, your PC's Subnet Mask should match the gateways subnet mask. The gateway has a default subnet mask of 255.255.255.0.

4. If this still does not work, press the reset button for 10 seconds. This will place the gateway into its factory default state. Go through the above procedure again.

5. Make sure NAT is enabled for your connection. If NAT is disabled the Gateway will not route frames correctly (except in Bridge connection).

The DSL Link LED continues to blink but does not go solid.

1. This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The main cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.

2. Verify that the phone line is connected directly to the wall and to the line input on the Gateway.

3. Make sure that for every parallel phone line connected to telephone or fax to install with a micro filter.

The DSL Link LED is always off.

1. Make sure you have DSL service. You should get some kind of information from your ISP that states that DSL service is installed. You can usually tell if the service is installed by listening to the phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.

2. Verify that the phone line is connected directly to the wall and to the line input on the Gateway. If the phone line is connected to the phone side of the Gateway or you have a splitter installed on the phone line, the DSL light will not come on.

If you can't solve your problems using the information sources mentioned above, please send us the problem description via http://www.corinex.com/web/com.nsf/Doc. We would like you to give us all possible information about your devices and your network, when contacting us. This includes:

- Types of devices you have, if possible with serial numbers (printed on the safety labels)
- Which of these devices are working incorrectly or don't work at all (indicate the problems)
- If it's possible, send us a scheme of your network topology also with the IP addresses for computers/router/access point, this can speed up the problem estimation. If you use any non-Corinex equipment, please specify what kind. The drawing can be made in any graphics editor, exported to one of the standard graphic formats (JPEG, GIF). Or you can just draw it on paper and scan it.
- Specify operating systems used with the devices.
- Please send us the firmware version and configuration of these devices. Please see the user guide for detailed instructions on this.

A.2 Frequently Asked Questions

What is the maximum number of IP addresses that the Gateway will support?
The Gateway will support up to 253 IP addresses.

Does the Gateway support IPX or AppleTalk?
No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications.
IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

Does the Internet connection of the Gateway support 100 Mbps Ethernet?
The Gateway's current hardware design supports up to 100 Mbps Ethernet on WAN port however, the Internet connection speed will vary depending on the speed of your broadband connection. The Gateway also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Gateway.

What is Network Address Translation and what is it used for?
Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Gateway to be used when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How can I block corrupted FTP downloads?
If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

If all else fails in the installation, what can I do?
Reset the Gateway by pressing the reset button (using a paper clip or pencil tip) and holding it for at least 10 secs, then release. At this point, the Wireless indicator and DSL indicator will turn off. The reset is in progress. When the Wireless indicator starts blinking, it means that the reset process is complete. The default settings are

then restored. Obtain and flash the latest firmware release that is readily available on the Corinex website, www.corinex.com.

How will I be notified of new firmware upgrades for the Gateway?
All Corinex firmware upgrades are posted on the Corinex website at www.corinex.com, where they can be downloaded for free. To upgrade the Gateway's firmware, use the Tools tab of the Gateway's web-based utility. If the Gateway's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Gateway firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Gateway function in a Macintosh environment?
Yes, but the Gateway's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the Appendices screen for the Gateway. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

Is the Gateway cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Gateway.

Does the Gateway pass PPTP packets or actively route PPTP sessions?
The Gateway allows PPTP packets to pass through.

What are the advanced features of the Gateway?
The Gateway's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing and DDNS.

Can the Gateway act as my DHCP server?
Yes. The Gateway has DHCP server software.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54 Mbps and an operating frequency of 2.4 GHz.

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?
When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

What is infrastructure mode?
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is ISM band?
The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?
Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission,

but the trade-off produces a signal that is, in effect, louder and thus easier to detect, rovided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS?

Direct-Sequence Spread- Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

Instant wireless products feature two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it generates security feature of scrambling. On the software side, instant wireless products offer the encryption function (WEP) to enhance security and access control. Users can set it up depending upon their needs. Can instant wireless products support file and printer sharing? Instant wireless products perform the same function as LAN products. Therefore, instant wireless products can work with NetWare, Windows NT/2000, or other LAN operating systems to support printer or file sharing.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I reset the Gateway to default?

Press the reset button on the rear panel of the Gateway (using a paper clip or pencil tip) and hold it for at least 10 secs, then release. At this point, the Wireless indicator and DSL indicator will turn off. The reset is in progress. When the Wireless indicator starts blinking, it means that the reset process is complete. The default settings are then restored.

How do I resolve issues with signal loss?
There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Gateway and a wireless PC will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Gateway and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment. You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.
WEP is probably enabled on the Gateway, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

How many channels/frequencies are available with the Gateway?
There are fourteen available channels, ranging from 1 to 14. For 802.11g we support 11 channels for North America, 13 for Europe (ETSI) and 14 for Japan.

How can your technology be beneficial in general?
General benefits are inexpensiveness, fastness and reliably manageable installation.

How can your technology be beneficial for me as Internet provider?
Our technology lowers the costs, and adds manageability.

How can your technology be beneficial for me as Internet user?
Lower the cost, reach points where there is no other alternative.

If your questions are not addressed here, refer to the Corinex website, www.corinex.com.

Appendix B Wireless Security

A Brief Overview

Whenever data - in the form of files, emails, or messages - is transmitted over your wireless network, it is open to attacks. Wireless networking is inherently risky because it broadcasts information on radio waves. Just like signals from your cellular or cordless phone can be intercepted, signals from your wireless network can also be compromised. What are the risks inherent in wireless networking? Read on.

What Are The Risks?

Computer network hacking is nothing new. With the advent of wireless networking, hackers use methods both old and new to do everything from stealing your bandwidth to stealing your data. There are many ways this is done, some simple, some complex. As a wireless user, you should be aware of the many ways they do this.

Every time a wireless transmission is broadcast, signals are sent out from your wireless PC or access point, but not always directly to its destination. The receiving PC or access point can hear the signal because it is within that radius. Just as with a cordless phone, cellular phone, or any kind of radio device, anyone else within that radius, who has their device set to the same channel or bandwidth can also receive those transmission.

Wireless networks are easy to find. Hackers know that, in order to join a wireless network, your wireless PC will typically first listen for “beacon messages”. These are identifying packets transmitted from the wireless network to announce its presence to wireless nodes looking to connect. These beacon frames are unencrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier) and the IP address of the network PC or access point. The SSID is analogous to the network’s name. With this information broadcast to anyone within range, hackers are often provided with just the information they need to access that network.

One result of this, seen in many large cities and business districts, is called “Warchalking”. This is the term used for hackers looking to access free bandwidth and free Internet access through your wireless network. The marks they chalk into the city streets are well documented in the Internet and communicate exactly where available wireless bandwidth is located for the taking.

Even keeping your network settings, such as the SSID and the channel, secret won't prevent a hacker from listening for those beacon messages and stealing that information. This is why most experts in wireless networking strongly recommend the use of WEP (Wired Equivalent Privacy). WEP encryption scrambles your wireless signals so they can only be recognized within your wireless network.

But even WEP has its problems. WEP's encryption algorithm is referred to as "simple", which also means "weak", because the technology that scrambles the wireless signal isn't too hard to crack for a persistent hacker.

There are five common ways that hackers can break into your network and steal your bandwidth as well as your data. The five attacks are popularly known as:

1. Passive Attacks
2. Jamming Attacks
3. Active Attacks
4. Dictionary-building or Table Attacks
5. Man-in-the-Middle Attacks

Passive Attacks

There's no way to detect a passive attack because the hacker is not breaking into your network. He is simply listening (eavesdropping, if you will) to the information your network broadcasts. There are applications easily available on the Internet that can allow a person to listen into your wireless network and the information it broadcasts. Information such as MAC addresses, IP addresses, usernames, passwords, instant message conversations, emails, account information, and any data transmitted wirelessly, can easily be seen by someone outside of your network because it is often broadcast in clear text. Simply put, any information transmitted on a wireless network leaves both the network and individual users vulnerable to attack. All a hacker needs is a "packet sniffer", software available on the Internet, along with other freeware or shareware hacking utilities available on the Internet, to acquire your WEP keys and other network information to defeat security.

Jamming Attacks

Jamming Attacks, when a powerful signal is sent directly into your wireless network, can effectively shut down your wireless network. This type of attack is not always intentional and can often come about simply due to the technology. This is especially possible in the 2.4 GHz frequency, where phones, baby monitors, and microwave ovens can create a great deal of interference and jam transmissions on your wireless network. One way to resolve this is by moving your wireless devices into the 5 GHz frequency, which is dedicated solely to information transmissions.

Active Attacks

Hackers use Active Attacks for three purposes: 1) stealing data, 2) using your network, and 3) modifying your network so it's easier to hack in the next time.

In an Active Attack, the hacker has gained access to all of your network settings (SSID, WEP keys, etc.) and is in your network. Once in your wireless network, the hacker has access to all open resources and transmitted data on the network. In addition, if the wireless network's access point is connected to a switch, the hacker will also have access to data in the wired network.

Further, spammers can use your Internet connection and your ISP's mail server to send tens of thousands of emails from your network without your knowledge.

Lastly, the hacker could make hacking into your network even easier by changing or removing safeguards such as MAC address filters and WEP encryption. He can even steal passwords and user names for the next time he wants to hack in.

Dictionary-Building or Table Attacks

Dictionary-building, or Table attacks, is a method of gaining network settings (SSID, WEP keys, etc.) by analyzing about a day's worth of network traffic, mostly in the case of business networks. Over time, the hacker can build up a table of network data and be able to decrypt all of your wireless transmissions. This type of attack is more effective with networks that transmit more data, such as businesses.

Man-in-the-Middle Attacks

A hacker doesn't need to log into your network as a user - he can appear as one of the network's own access points, setting himself up as the man-in-the-middle. To do this, the hacker simply needs to rig an access point with your network's settings and send out a stronger signal that your access point. In this way, some of your network's PCs may associate with this rogue access point, not knowing the difference, and may begin sending data through it and to this hacker.

The trade-off for the convenience and flexibility wireless networking provides is the possibility of being hacked into through one of the methods described here. With wireless networks, even with WEP encryption, open to the persistent hacker, how can you protect your data? The following section will tell you how to do just that.

B.1 Maximizing Wireless Security

Security experts will all tell you the same thing: Nothing is guaranteed. No technology is secure by itself. An unfortunate axiom is that building the better mousetrap can often create a better mouse. This is why, in the examples below, your implementation and administration of network security measures is the key to maximizing wireless security.

No preventative measure will guarantee network security but it will make it more difficult for someone to hack into your network. Often, hackers are looking for an easy target. Making your network less attractive to hackers, by making it harder for them to get in, will make them look elsewhere.

How do you do this? Before discussing WEP and WPA, let's look at a few security measures often overlooked.

A. Common Sense Solutions

1) Network Content

Now that you know the risks assumed when networking wirelessly, you should view wireless networks as you would the Internet. Don't host any systems or provide access to data on a wireless network that you wouldn't put on the Internet.

2) Network Layout

When you first lay out your network, keep in mind where your wireless PCs are going to be located and try to position your access point(s) towards the center of that network radius. Remember that access points transmit indiscriminately in a radius; placing an access point at the edge of the physical network area reduces network performance and leaves an opening for any hacker smart enough to discover where the access point is transmitting.

This is an invitation for a man-in-the-middle attack, as described in the previous section. To perform this type of attack, the hacker has to be physically close to your network. So, monitoring both your network and your property is important. Furthermore, if you are suspicious of unauthorized network traffic, most wireless products come with a log function, with which you can view activity on your network and verify if any unauthorized users have had access.

3) Network Devices

With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. If they get into the hands of a hacker, so do all of your settings. So keep an eye on them.

4) Administrator passwords

Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

5) SSID

There are a few things you can do to make your SSID more secure:

a. Disable Broadcast
b. Make it unique
c. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. This is a option for convenience, allowing anyone to log into your wireless network. In this case, however, anyone includes hackers. So don't broadcast the SSID.

A default SSID is set on your wireless devices by the factory. (The Corinex default SSID is "corinex".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Changing your SSID regularly will force any hacker attempting to gain access to your wireless network to start looking for that new SSID.

With these three steps in mind, please remember that while SSIDs are good for segmenting networks, they fall short with regards to security. Hackers can usually find them quite easily.

6) MAC addresses

Enable MAC address filtering if your wireless products allow it. MAC address filtering will allow you to provide access to only those wireless nodes with certain MAC addresses. This makes it harder for a hacker using a random MAC address or spoofing (faking) a MAC address.

7) Firewalls

Once a hacker has broken into your wireless network, if it is connected to your wired network, they'll have access to that, too. This means that the hacker has effectively used your wireless network as a backdoor through your firewall, which you've put in place to protect your network from just this kind of attack via the Internet.

You can use the same firewall technology to protect your wired network from hackers coming in through your wireless network as you did for the Internet. Rather than connecting your access point to an unprotected switch, swap those out for a router with a built-in firewall. The router will show the access point coming in through its WAN port and its firewall will protect your network from any transmissions entering via your wireless network. PCs unprotected by a firewall router should at least run firewall software, and all PCs should run up-to-date antiviral software.

B. WEP

Wired Equivalent Privacy (WEP) is often looked upon as a panacea for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

Programs exist on the Internet that are designed to defeat WEP. The best known of these is AirSnort. In about a day, AirSnort can analyze enough of the wireless transmissions to crack the WEP key. Just like a dictionary-building attack, the best prevention for these types of programs is by not using static settings, periodically changing WEP keys, SSID, etc.

There are several ways that WEP can be maximized:

a) Use the highest level of encryption possible
b) Use multiple WEP keys
c) Change your WEP key regularly

Current encryption technology offers 64-bit and 128-bit WEP encryption. If you are using 64-bit WEP, swap out your old wireless units for 128-bit encryption right away. Where encryption is concerned, the bigger and more complex, the better. A WEP key is a string of hexadecimal characters that your wireless network uses in two ways. First, nodes in your wireless network are identified with a common WEP key. Second, these WEP keys encrypt and decrypt data sent over your wireless network. So, a higher level of security ensures that hackers will have a harder time breaking into your network.

Setting one, static WEP key on your wireless network leaves your network open the threats even as you think it is protecting you. While it is true that using a WEP key increases wireless security, you can increase it further by using multiple WEP keys.

Keep in mind that WEP keys are stored in the firmware of wireless cards and access points and can be used to hack into the network if a card or access point falls into the wrong hands. Also, should someone hack into your network, there would be nothing preventing someone access to the entire network, using just one static key.

The solution, then, is to segment your network up into multiple groups. If your network had 80 users and you used four WEP keys, a hacker would have access to only ¼ of your wireless network resources. In this way, multiple keys reduce your liability.

Finally, be sure to change your WEP key regularly, once a week or once a day. Using a “dynamic” WEP key, rather than one that is static, makes it even harder for a hacker to break into your network and steal your resources.

C. WPA

Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

Appendix C Glossary

10BaseT - An Ethernet standard that uses twisted wire pairs. 100BaseTX - IEEE physical layer specification for 100 Mbps over two pairs of Category 5 UTP or STP wire.

1000BASE-T - A 100 Mbps technology based on the Ethernet/CD network access method. Provides half-duplex (CSMA/CD) and full-duplex 1000 Mbps Ethernet service over Category 5 links as defined by ANSI/TIA/EIA-568-A. Topology rules for 1000BASE-T are the same as those used for 100BASE-T. Category 5 link lengths are limited to 100 meters by the ANSI/TIA/EIA-568-A cabling standard. Only one CSMA/CD repeater will be allowed in a collision domain.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11 Mbps and an operating frequency of 2.4 GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54 Mbps, an operating frequency of 2.4 GHz, and backward compatibility with 802.11b devices.

Access Point - Device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card (NIC) is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

Asymmetrical Digital Subscriber Line (ADSL) - A new standard for transmitting at speeds up to 7 Mbps over a single copper pair.

Auto-negotiate - To automatically determine the correct settings. The term is often used with communications and networking. For example, Ethernet 10/100 cards, hubs, and switches can determine the highest speed of the node they are connected to and adjust their transmission rate accordingly.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone – The part of a network that connects most of the systems and networks together and handles the most data.

Bandwidth – 1. Measure of the information capacity of a transmission channel, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps). 2. The difference between the highest and lowest frequencies of a band that can be passed by a transmission medium without undue distortion, such as the AM band 535 to 1705 kilohertz.

Baseband - Transmission scheme in which the entire bandwidth, or data-carrying capacity, of a medium (such as a coaxial cable) is used to carry a single digital pulse, or signal, between multiple users. Because digital signals are not modulated, only one kind of data can be transmitted at a time. Contrast with broadband.

Baud (Bite at Unit Density) - A measure of the speed of transmission of data; number of elements transmitted per second.

Beacon Interval - The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit – A binary digit. The value—0 or 1—used in the binary numbering system. Also, the smallest form of data.

Boot – To cause the computer to start executing instructions. Personal computers contain built-in instructions in a ROM chip that are automatically executed on startup. These instructions search for the operating system, load it, and pass control to it.

Bridge/Router- A device that can provide the functions of a bridge, router, or both concurrently. Bridge/router can route one or more protocols, such as TCP/IP and/or XNS, and bridge all other traffic.

Broadband - A data-transmission scheme in which multiple signals share the bandwidth of a medium. This allows the transmission of voice, data, and video signals over a single medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

Broadcast Domain - Defines the set of all devices which will receive broadcast frames originating from any device within the set. Broadcast domains are normally bounded by routers.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

Buffer - A storage area used for handling data in transit. Buffers are often used to compensate for differences in processing speed between network devices.

Byte - The fundamental unit that a computer uses in its operation. It is a group of adjacent binary digits, usually 8, often used to represent a single character.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet. Once connected, cable modem users have a continuous connection to the Internet. Cable modems feature asymmetric transfer rates: around 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

Caching – 1. Speeds information processing by storing information from a transaction to use for later transactions. 2. Storing or buffering data in a temporary location, so that the information can be retrieved quickly by an application program.

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) - A method of data transfer that is used to prevent data loss in a network.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) - A channel access mechanism wherein devices wishing to transmit first check the channel for a carrier. If no carrier is sensed for some period of time, devices can transmit. If two devices transmit simultaneously, a collision occurs and is detected by all colliding devices, which subsequently delays their retransmissions for some random length of time. CSMA/CD access is used by Ethernet /IEEE 802.3 and HomePlug.

CAT 3 - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify "categories" (the singular is commonly referred to as "CAT") of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 3 cable has a maximum throughput of 16 Mbps and is usually utilized for 10BaseT networks.

CAT 5 - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify "categories" (the singular is commonly referred to as "CAT") of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

CAT 5e - The additional cabling performance parameters of return loss and farend crosstalk (FEXT) specified for 1000BASE-T and not specified for 10BASE-T and 100BASE-TX are related to differences in the signaling implementation. 10BASE-T and 100BASE-TX signaling is unidirectional—signals are transmitted in one direction on a single wire pair. In contrast, Gigabit Ethernet is bi-directional—signals are transmitted simultaneously in both directions on the same wire pair; that is, both the transmit and receive pair occupy the same wire pair.

CPU (Central Processing Unit) - The computing part of the computer. Also called the "processor," it is made up of the control unit and ALU.

Daisy Chain - Connected in series, one after the other. Transmitted signals go to the first device, then to the second, and so on.

Database - A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.

Data Packet - One frame in a packet-switched message. Most data communications is based on dividing the transmitted message into packets. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

Demodulation - Opposite of modulation; the process of retrieving data from a modulated carrier wave.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network. DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DMZ - (DeMilitarized Zone) allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP address if you want to use DMZ Hosting.

DNS - Domain Name System (DNS). The distributed name/address mechanism used in the Internet.

Domain - A subnetwork comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Download - To receive a file transmitted over a network. In a communications session, download means receive, and upload means transmit.

DSL - (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

Driver - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network-compatible client or server operating system.

DSSS (Direct-Sequence Spread-Spectrum) - DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

DTIM - (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

Dynamic Routing - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

Encapsulation - The wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit.

Encryption - Applying a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading information. Decryption applies the algorithm in reverse to restore the data to its original form.

Ethernet - A baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks operate at 10 Mbps using CSMA/CD to run over coaxial cable. Ethernet is similar to a series of standards produced by IEEE referred to as IEEE 802.3.

Fast Ethernet - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

Firewall - A firewall is a set of related programs, located at a network gateway server, which protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access. Basically, a firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination.

Firmware - Programming that is inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) – 1. An IP application protocol for transferring files between network nodes. 2. An Internet protocol that allows a user on one host to transfer files to and from another host over a network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A system that interconnects networks.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A utility that provides for querying, defining and managing IP addresses within a network. A commonly used utility, under Windows NT and 2000, for configuring networks with static IP addresses.

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

IRQ (Interrupt ReQuest) - hardware interrupt on a PC. There are 16 IRQ lines used to signal the CPU that a peripheral event has started or terminated. Except for PCI devices, two devices cannot use the same line.

ISM band - Radio band used in wireless networking transmissions.

ISP - An ISP (Internet service provider) is a company that provides individuals and companies access to the Internet and other related services such as website-building and virtual hosting.

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

Latency - The time delay between when the first bit of a packet is received and the last bit is forwarded.

MAC Address - The MAC (Media Access Control) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Mbps (MegaBits Per Second) - One million bits per second; unit of measurement for data transmission.

Multicasting - Sending data to a group of destinations at once.

NAT - NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

NetBEUI (NetBIOS Extended User Interface) - The transport layer for NetBIOS. NetBIOS and NetBEUI were originally part of a single protocol suite that was later separated. NetBIOS sessions can be transported over NetBEUI, TCP/IP, and SPX/IPX protocols.

NetBIOS - The native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI), NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and IPX/SPX, which are routable protocols. NetBIOS computers are identified by a unique 15-character name, and Windows machines (NetBIOS machines) periodically broadcast their names over the network so that Network Neighborhood can catalog them. For TCP/IP networks, NetBIOS names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server. There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.

Network - A system that transmits any combination of voice, video, and/or data between users.

Network Mask - also known as the "Subnet Mask."

NIC (Network Interface Card) - A board installed in a computer system, usually a PC, to provide network communication capabilities to and from that computer system. Also called an adapter.

Node - A network junction or connection point, typically a computer or work station.

Notebook (PC) - A notebook computer is a battery-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, at temporary offices, and at meetings. A notebook computer, sometimes called a laptop computer, typically weighs less than five pounds and is three inches or less in thickness.

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

Packet - A unit of data sent over a network.

Packet Filtering - Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.)

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Corinex products.

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Plug-and-Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

Port - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems, and printers.

Port Mirroring - Port mirroring, also known as a roving analysis port, is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely.

PPPoE (Point to Point Protocol over Ethernet) - A method used mostly by DSL providers for connecting personal computers to a broadband modem for Internet access. It is similar to how a dial-up connection works but at higher speeds and quicker access.

PPTP (Point-to-Point Tunneling Protocol) - A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

Preamble - Part of the wireless signal that synchronizes network traffic.

Print Server - A hardware device that enables a printer to be located anywhere in the network.

RIP (Routing Information Protocol) - A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers and is known to waste bandwidth. AppleTalk, DECnet, TCP/IP, NetWare, and VINES all use incompatible versions of RIP.

RJ-11 (Registered Jack-11) - A telephone connector that holds up to six wires. The RJ-11 is the common connector used to plug a telephone into a wall.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Router - A networking device that connects multiple networks together, such as a local network and the Internet.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program." The two major categories of software are "system software" and "application software." System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user. A common misconception is that software is data. It is not. Software tells the hardware how to process the data.

SOHO (Small Office/Home Office) - Market segment of professionals who work at home or in small offices.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set IDentifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

Storage - The semi-permanent or permanent holding place for digital data.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

Swapping - Replacing one segment of a program in memory with another and restoring it back to the original when required.

Switch - 1. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (Transmission Control Protocol) - A method (protocol) used along with the Internet Protocol (Internet Protocol) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP/IP - Transmission Control Protocol/Internet Protocol (TCP/IP) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one place to another in a given time period.

Topology - A network's topology is a logical characterization of how the devices on the network are connected and the distances between them. The most common network devices include hubs, switches, routers, and gateways. Most large networks contain several levels of interconnection, the most important of which include edge connections, backbone connections, and wide-area connections.

TX Rate – Transmission Rate.

UDP (User Datagram Protocol) - A communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To send a file transmitted over a network. In a communications session, upload means transmit, and download means receive.

URL (Uniform Resource Locator) - The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

UTP - Unshielded twisted pair is the most common kind of copper telephone wiring. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable.

VLAN (Virtual LAN) - A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

Virtual Server - Multiple servers that appear as one server, or one system image, to the operating system or for network administration.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN - A communications network that covers a wide geographic area, such as a state or country.

WEP (Wired Equivalent Privacy) - A data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11 standard.

WINIPCFG - Configuration utility based on the Win32 API for querying, defining, and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

Workgroup - Two or more individuals that share files and databases.

Appendix D: How to Ping Your ISP's Email and Web Addresses

Virtually all Internet addresses are configured with words or characters (e.g., www.corinex.com, www.yahoo.com, etc.) However, recently these Internet addresses are assigned to IP addresses, which are the true addresses on the Internet. For example, www.corinex.com is recently 81.0.193.56 at the time of producing this manual. If you type this address into your web browser, you will end up at the Corinex home page every time.

Some servers translate the URL to an IP address, so called DNS (Domain Name System) Servers. However, IP and web addresses can be long and hard to remember sometimes. From this reason, certain ISPs will shorten their server addresses to single words or codes on their users' web browser or e-mail configurations. If your ISP's email and web server addresses are configured with single words (www, e-mail, home, pop3, etc.) rather than entire Internet addresses or IP addresses, the Access Point may have problems by sending or receiving mail and by accessing the Internet.

The solution is to determine the true web addresses behind your ISPs code words. You can determine the IP and web addresses of your ISP's servers by "pinging" them.

Important: If you don't have your ISP's web and e-mail IP addresses, you must either get them from your ISP or follow these steps prior to connecting your *Corinex ADSL2+ Wireless Gateway G* to your network.

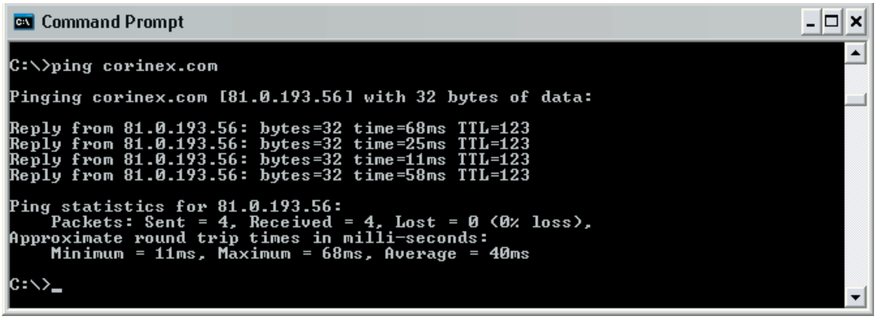
D.1 Step One: Pinging an IP Address

The first step to determining your ISP's web and e-mail server address is to ping its IP address.

1. Power on the computer and the Gateway, and restore the network configuration set by your ISP if you have changed it.

2. Click **Start**, then **Run**, and type **command**. This will bring up the DOS window.

3. At DOS command prompt, type **ping corinex.com** (assuming that your desired IP address location is configured as corinex.com) and press **Enter**. As an exam ple, the following data information, taken from a ping of Microsoft Network e-mail server, will be displayed:



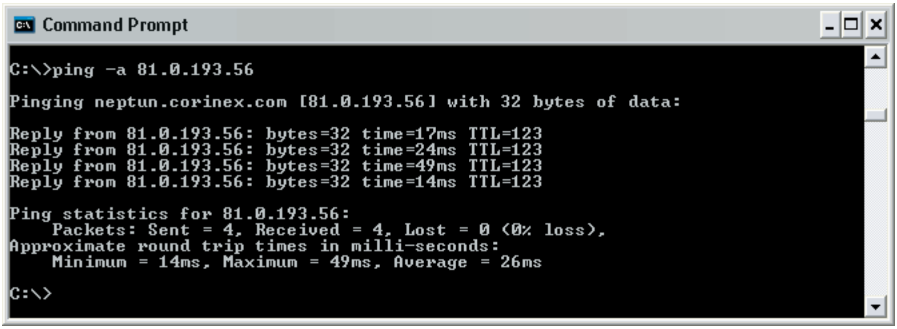
```
C:\>ping corinex.com

Pinging corinex.com [81.0.193.56] with 32 bytes of data:

Reply from 81.0.193.56: bytes=32 time=68ms TTL=123
Reply from 81.0.193.56: bytes=32 time=25ms TTL=123
Reply from 81.0.193.56: bytes=32 time=11ms TTL=123
Reply from 81.0.193.56: bytes=32 time=58ms TTL=123

Ping statistics for 81.0.193.56:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 68ms, Average = 40ms

C:\>_
```

4. Write down the IP address returned by the ping command. (In the example above: 81.0.193.56) This IP address is the actual IP address of the mail server, or any other value you have pinged.

D.2 Step Two: Pinging for a Web Address

While the above-mentioned IP address could perform as your e-mail server address, it might not be permanent. IP addresses change very much often. Web addresses, however, usually don’t. This is the reason, why you are likely to have fewer problems by configuring your system with web addresses rather than IP addresses. Follow the instructions below to find the web address assigned to the IP address you just pinged.

1. At the DOS command prompt, type ping **-a 81.0.193.56**, where 81.0.193.56 is the IP address you just pinged. Information such as the following data will be displayed.



```
C:\>ping -a 81.0.193.56

Pinging neptun.corinex.com [81.0.193.56] with 32 bytes of data:

Reply from 81.0.193.56: bytes=32 time=17ms TTL=123
Reply from 81.0.193.56: bytes=32 time=24ms TTL=123
Reply from 81.0.193.56: bytes=32 time=49ms TTL=123
Reply from 81.0.193.56: bytes=32 time=14ms TTL=123

Ping statistics for 81.0.193.56:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 49ms, Average = 26ms

C:\>
```

2. Write down the web address returned by the ping command (In the example on previous picture corinex.com is the web address). This web address is the web address assigned to the IP address you just pinged. While the IP address of mail could change conceivably, it is presumably that this web address will not.

3. Replace your ISP's abbreviated server address with this extended web address in the corresponding Internet application (web browser, e-mail application, etc.).

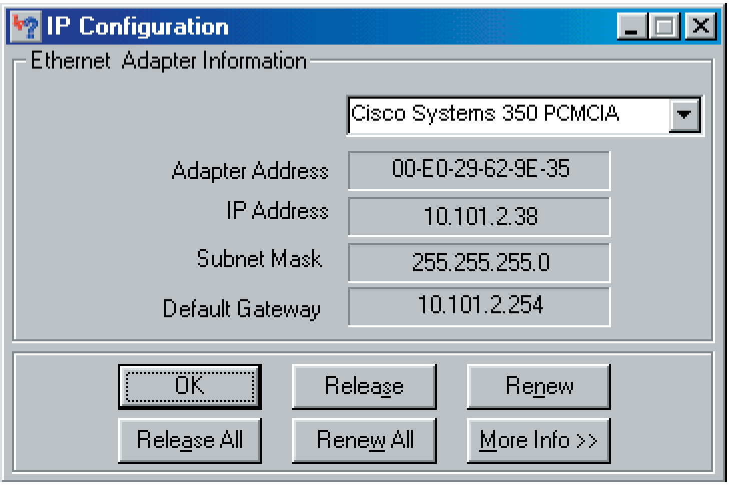
Once you have replaced the brief server address with the true server address, the Gateway should have no problem accessing the Internet through this Internet application.

Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter

This section describes how to find the MAC address of your Ethernet adapter of your computer to do either MAC Filtering or MAC Address Cloning for the Router and ISP. You can also find the IP address of your computer's Wireless or Ethernet adapter. The IP address is used for filtering, forwarding, and DMZ. In this appendix follow the next steps to find the MAC address or IP address for your adapter of your Windows 95, 98, Me, NT, 2000, XP, Linux or Macintosh Computer.

E.1 For Windows 95, 98, and ME:

1. Click **Start** and **Run**. In the Open field, enter **winipcfg**, as shown on the following picture. Then press the **Enter** key or the **OK** button.



IP Configuration

Ethernet Adapter Information

Cisco Systems 350 PCMCIA

Adapter Address: 00-E0-29-62-9E-35

IP Address: 10.101.2.38

Subnet Mask: 255.255.255.0

Default Gateway: 10.101.2.254

2. When the IP Configuration window appears, select the Wireless, Ethernet adapter or USB network adapter you are using to connect to the *Corinex ADSL2+ Wireless Gateway G* via Ethernet, Wireless or USB.

3. Write down the Adapter Address as shown on your computer screen. This is the MAC address for your Wireless, Ethernet adapter or USB network adapter and will be shown as a series of numbers and letters. The MAC address/Adapter Address is what you will use for MAC Address Cloning or MAC Address Filtering.

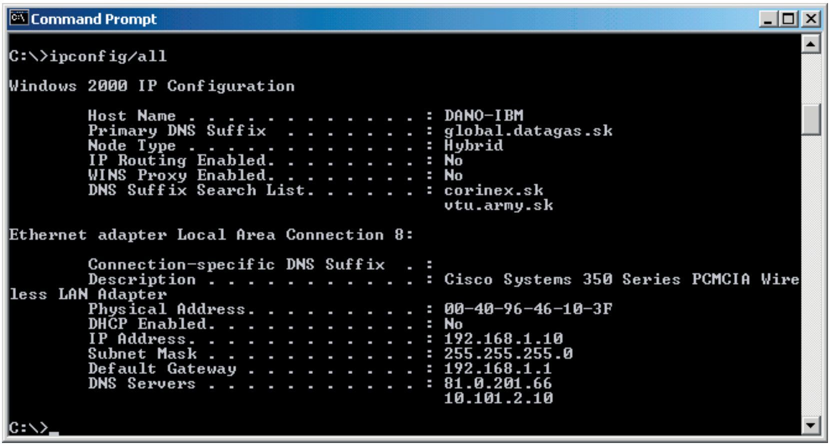
This example shows the IP address of your Wireless adapter as 10.101.2.38. Your computer may show something different.

E.2 For Windows NT, 2000, and XP:

The following steps show an alternative way of obtaining the MAC and IP address for your Wireless or Ethernet adapter.

1. Click **Start** and **Run**. In the Open field, enter **cmd**. Press **Enter** key or click the **OK** button.

2. In the command prompt, enter **ipconfig /all**. Then press **Enter** key.



```
C:\>ipconfig/all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : DANO-IBM
        Primary DNS Suffix  . . . . . . . : global.datagas.sk
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : corinex.sk
                                            vtu.army.sk

Ethernet adapter Local Area Connection 8:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Cisco Systems 350 Series PCMCIA Wire
less LAN Adapter
        Physical Address. . . . . . . . . : 00-40-96-46-10-3F
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 81.0.201.66
                                            10.101.2.10

C:\>_
```

3. Write down the Physical Address as shown on your computer screen (see previous picture); it is the MAC address for your Wireless or Ethernet adapter. This will appear as a series of letters and numbers. The MAC address/Physical Address is what you will use for MAC Address Cloning or MAC Filtering.

The example on previous picture shows the IP address of your Wireless adapter as 192.168.1.10. Your computer might show something different.

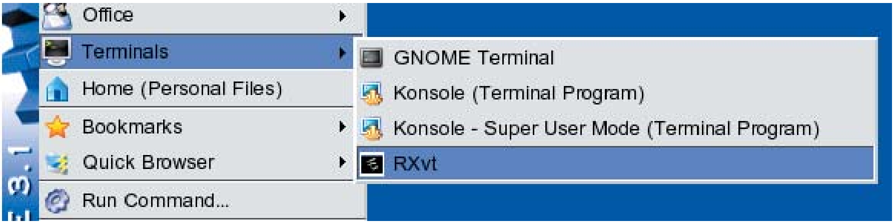
Note: The MAC address is also called Physical Address.

When entering the information using the Access Point's web-based utility, you will type the 12-digit MAC address in this format, XX:XX:XX:XX:XX:XX without the hyphens for MAC Filtering.

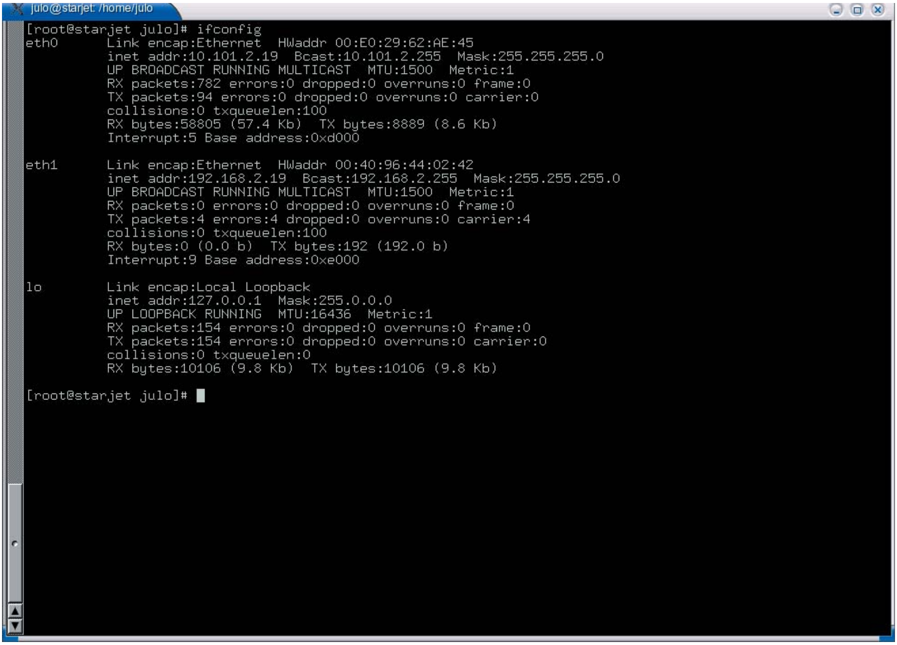
When entering information for MAC Address Cloning, type the 12-digit MAC address.

E.3 For Linux PC:

From the **Start** Button on Desktop bar, choose **Terminals->Xterm** (or any other convenient terminal).

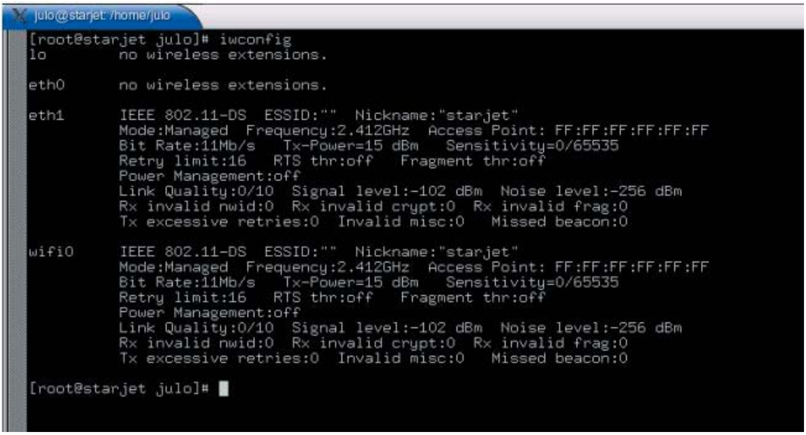


Login as superuser by issuing **su** command, then press **Enter**. Provide the password, and press **Enter**. Enter **ifconfig**, press **Enter**. In the field Hwaddr is the requested MAC Address.



```
[root@starjet julo]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:E0:29:62:AE:45
          inet addr:10.101.2.19  Bcast:10.101.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:782 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:58805 (57.4 Kb)  TX bytes:8889 (8.6 Kb)
          Interrupt:5 Base address:0xd000

eth1      Link encap:Ethernet  HWaddr 00:40:96:44:02:42
          inet addr:192.168.2.19  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:4 dropped:0 overruns:0 carrier:4
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:192 (192.0 b)
          Interrupt:9 Base address:0xe000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:154 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10106 (9.8 Kb)  TX bytes:10106 (9.8 Kb)

[root@starjet julo]# █
```

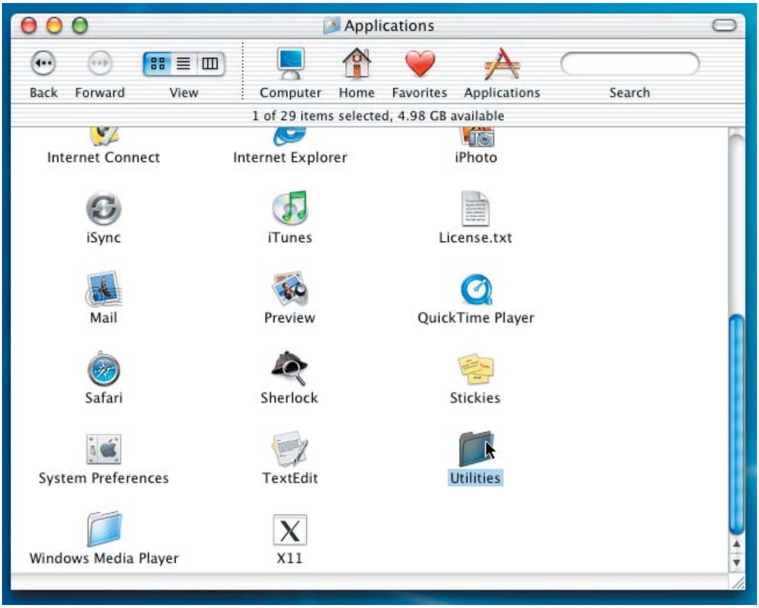
Login as superuser, by issuing **su** command, and then press **Enter**. Provide the password, and press **Enter** again. Enter **iwconfig**, and then press **Enter**. You can see the wireless port parameters.



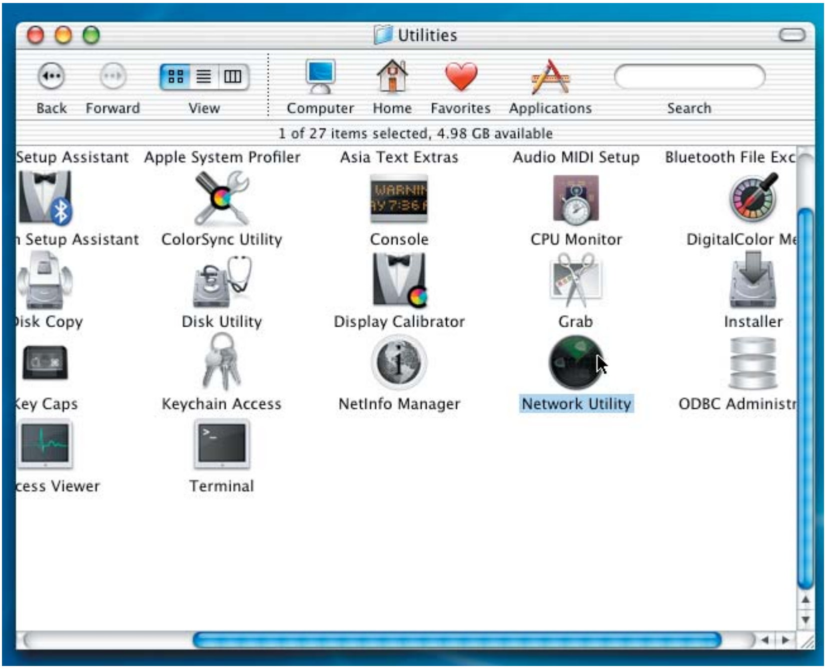
```
[root@starjet julo]# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      IEEE 802.11-DS  ESSID:""  Nickname:"starjet"
          Mode:Managed  Frequency:2.412GHz  Access Point: FF:FF:FF:FF:FF:FF
          Bit Rate:11Mb/s   Tx-Power=15 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0/10  Signal level:-102 dBm  Noise level:-256 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

wifi0     IEEE 802.11-DS  ESSID:""  Nickname:"starjet"
          Mode:Managed  Frequency:2.412GHz  Access Point: FF:FF:FF:FF:FF:FF
          Bit Rate:11Mb/s   Tx-Power=15 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0/10  Signal level:-102 dBm  Noise level:-256 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

[root@starjet julo]# █
```

E.4 For Macintosh OS X computer:

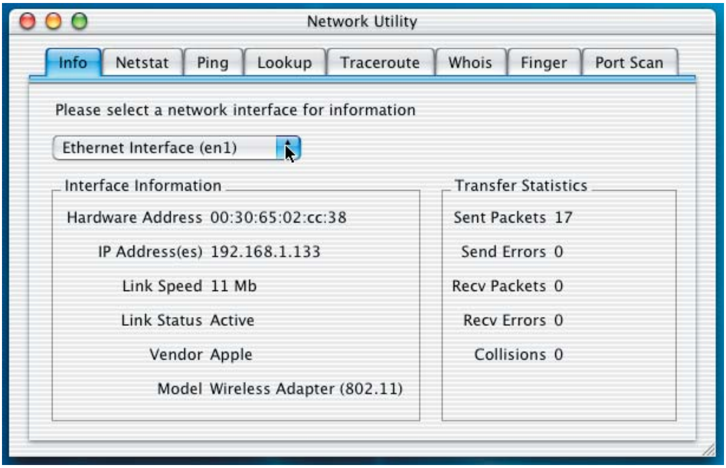
1. In **Applications** open **Utilities**.



2. In **Utilities** select **Network Utility**.



3. Select the interface connected to the *Corinex ADSL2+ Wireless Gateway G* through the Ethernet or through the Wireless. In this section you can see the wireless connection type.



Please select a network interface for information

Ethernet Interface (en1)

Interface Information

Hardware Address 00:30:65:02:cc:38

IP Address(es) 192.168.1.133

Link Speed 11 Mb

Link Status Active

Vendor Apple

Model Wireless Adapter (802.11)

Transfer Statistics

Sent Packets 17

Send Errors 0

Recv Packets 0

Recv Errors 0

Collisions 0

4. The field **Hardware Address** contains the MAC Address of the selected interface.