



# NexusLink 5700

## Wireless ADSL bonding IAD

### User's Manual

Version C1.0, October 5, 2010

---



## **Warning**

- Before servicing or disassembling this equipment, always disconnect all power and telephone lines from the device.
- Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is clearly stated in [Appendix C](#).

## **Preface**

This manual provides information to network administrators. It covers the installation, operation and applications of the Wireless ADSL bonding IAD. The individual reading this manual is presumed to have a basic understanding of telecommunications.

This document is subject to change without notice. For product update, new product release, manual revision, software upgrade, technical support, etc., visit Comtrend Corporation at <http://www.comtrend.com>

## **FCC Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

<p><b>FCC Caution:</b> The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.</p>
--

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.

### **FCC Radiation Exposure Statement**

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body

### **Copyright**

Copyright© 2010 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without the prior written consent of Comtrend Corporation.

### **Technical support**

If you find the product to be inoperable or malfunctioning, please contact a technical support engineer for immediate service by email at [INT-support@comtrend.com](mailto:INT-support@comtrend.com)

### **Save Our Environment**



This symbol means that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations.

Never throw-out this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for instructions from your municipal government on how to correctly dispose of it. Please be responsible and protect our environment.

# Table of Contents

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>6</b>
1.1 FEATURES .....	6
1.2 APPLICATION .....	7
1.3 FRONT PANEL LED INDICATORS .....	8
<b>CHAPTER 2 INSTALLATION .....</b>	<b>9</b>
2.1 HARDWARE INSTALLATION .....	9
<b>CHAPTER 3 LOGIN VIA WEB BROWSER .....</b>	<b>10</b>
3.1 IP ADDRESS .....	10
3.2 LOGIN PROCEDURE.....	11
<b>CHAPTER 4 DEVICE .....</b>	<b>12</b>
4.1 DEVICE SUMMARY .....	13
4.2 RESET STATISTICS.....	14
4.3 TROUBLESHOOT .....	15
4.4 WIRELESS .....	17
4.4.1 <i>Enable Wireless</i> .....	19
4.4.2 <i>Wireless - Security Configure</i> .....	19
4.4.3 <i>WPS Setup</i> .....	22
4.4.4 <i>Wireless - Advanced Configure</i> .....	26
4.5 RESTART YOUR SYSTEM .....	28
4.6 HOME NETWORK.....	30
4.7 GAMING AND APPLICATIONS.....	32
4.7.1 <i>Incoming Traffic Control</i> .....	33
4.7.2 <i>Outgoing Traffic Control</i> .....	35
4.8 RESET ACCESS CODE.....	37
<b>CHAPTER 5 BROADBAND.....</b>	<b>39</b>
5.1 STATUS .....	39
5.2 CONFIGURE .....	40
<b>CHAPTER 6 HOME NETWORK.....</b>	<b>42</b>
6.1 LAN STATUS .....	42
6.2 CONFIGURE .....	43
6.3 WIRELESS STATUS .....	48
6.4 WIRELESS CONFIGURE .....	49
6.5 WIRELESS MAC FILTER .....	50
<b>CHAPTER 7 VOIP.....</b>	<b>52</b>

7.1 STATUS .....	53
7.2 SIP .....	53
7.2.1 <i>Global Parameters</i> .....	54
7.2.2 <i>Service Provider</i> .....	55
7.3 RTCP .....	57
7.3.1 <i>Global Parameters</i> .....	57
7.3.2 <i>Service Provider</i> .....	58
7.4 TELEPHONE CALLS .....	59
<b>CHAPTER 8 FIREWALL .....</b>	<b>59</b>
8.1 STATUS .....	61
8.2 INBOUND FILTER .....	61
8.3 OUTBOUND FILTER .....	61
8.4 PORT FORWARDING.....	62
8.5 PORT TRIGGERING .....	65
<b>CHAPTER 9 MAINTENANCE.....</b>	<b>67</b>
9.1 TEST .....	67
9.2 DSL.....	68
9.2.1 <i>xDSL BER Test</i> .....	69
9.2.2 <i>Reset Statistics</i> .....	71
9.2.3 <i>Draw Graph Tone</i> .....	71
9.2.4 <i>Draw Loss of Signal Graph</i> .....	72
9.2.5 <i>Draw Loss of Frames Graph</i> .....	72
9.2.6 <i>Loss of Power</i> .....	73
9.3 PING/TRACEROUTE/NSLOOKUP .....	74
9.3.1 <i>Ping</i> .....	74
9.3.2 <i>TraceRoot</i> .....	75
9.3.3 <i>NSLookup</i> .....	75
9.4 SYSTEM LOG .....	76
9.4.1 <i>Refresh</i> .....	77
9.4.2 <i>Export Syslog</i> .....	77
9.5 PASSWORD.....	79
9.5.1 <i>Use New Access Code</i> .....	80
9.5.2 <i>Clear Input</i> .....	80
9.5.3 <i>Reset to Default Access Code</i> .....	80
9.6 UPGRADE.....	81
9.7 REBOOT.....	82
9.8 FACTORY RESET .....	83

<b>APPENDIX A: FIREWALL .....</b>	<b>85</b>
<b>APPENDIX B: PIN ASSIGNMENTS.....</b>	<b>89</b>
<b>APPENDIX C: SPECIFICATIONS.....</b>	<b>90</b>
<b>APPENDIX D: SSH CLIENT .....</b>	<b>93</b>

# Chapter 1 Introduction

The NexusLink 5700 Wireless ADSL bonding IAD features flexible networking connectivity with dual ADSL line capability, four 10/100 Ethernet ports, and an 802.11g wireless LAN access point. It has robust routing capabilities to segment and direct data streams and allows for multiple data encapsulations.

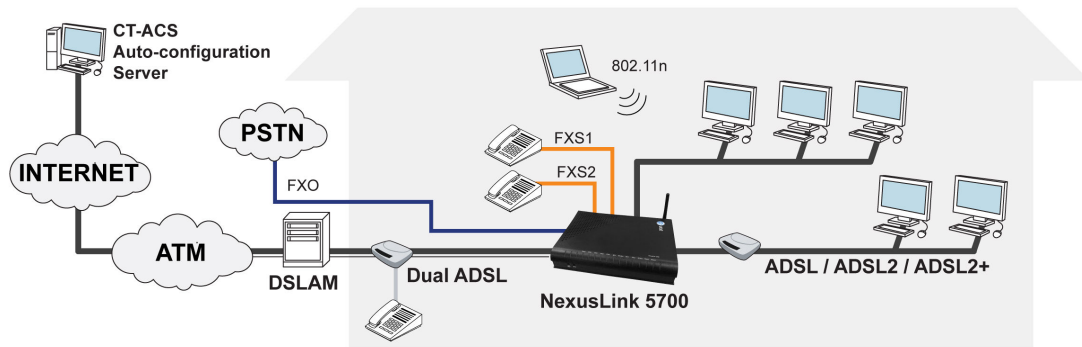
The NexusLink 5700 is a black box solution for deploying Triple Play architectures, doubling bandwidth (48Mbps) performance over traditional ADSL2 modems. It provides higher level performance with embedded security, QoS, VPN and remote management functions. As an added bonus, the USB host acts as a printer hub and will enable future product enhancements available by software upgrade.

## 1.1 Features

- NexusLink 5700 (Annex M)
- Dual ADSL2 PTM bonded
- Wi-Fi Support
- UPnP installation
- Integrated 802.11b/g/n
- WPA and 802.1x
- RADIUS client
- IP /MAC address filtering
- Static route/RIP/RIP v2 routing functions
- Dynamic IP assignment
- NAT/PAT
- IGMP Proxy and fast leave
- DHCP Server/Relay/Client
- DNS Relay
- Supports 16 VCs
- Embedded SNMP agent
- Web-based management
- Remote configuration and upgrade
- Supports TR-069/TR-098/TR-104/TR-111 For Remote Management
- Configuration backup and restoration
- FTP server
- TFTP server

## 1.2 Application

This diagram depicts the application of the NexusLink 5700 on a wireless network.





## 1.3 Front Panel LED Indicators

The front panel LED indicators are shown in the picture below, followed by an explanation in the table below.

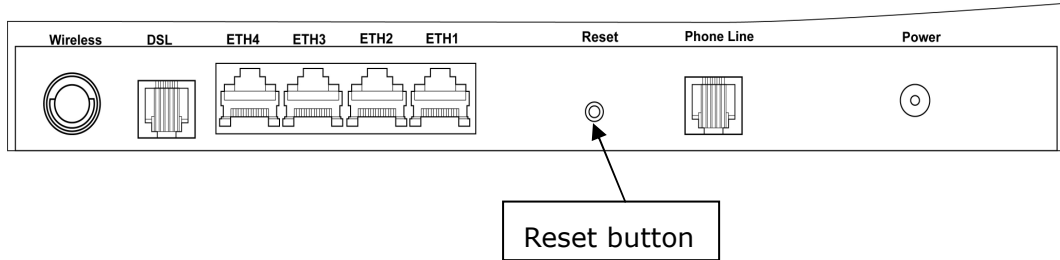


LED	Color	Mode	Function
<b>POWER</b>	Green	On	The router is powered up.
		Off	The router is powered down.
<b>LAN 1X~4X</b>	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
	Blink	Data transmitting or receiving over LAN.	
<b>WPS</b>	Green	On	WPS mode exists protected clients
		Blink	WPS mode is on for 120 seconds
	Off	WPS mode is off	
<b>WIRELESS</b>	Green	On	The Wireless is ready and idle.
		Off	The Wireless is not installed.
	Blink	Data transmitting or receiving over Wireless	
<b>DSL1~DSL2</b>	Green	On	The DSL link is established.
		Off	The DSL link is not established.
	Blink	The DSL link is training.	
<b>Service</b>	Green	On	The Internet link (PVC) is established.
		Off	The Internet link (PVC) is not established.
<b>Phone1</b>	Green	On	The FXS phone 1 is off hook.
		Off	The FXS phone 1 is on hook.
<b>Phone2</b>	Green	On	The FXS phone 2 is off hook.
		Off	The FXS phone 2 is on hook.

# Chapter 2 Installation

## 2.1 Hardware Installation

Follow the instructions below to complete the hardware installation. A schematic of the back of the router is shown below for reference.



### Connection to Power

Connect the power jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source. After all connections have been made the router will perform a self-test. Wait a few moments and the router will be ready to operate.

---

**Caution 1:** If the router fails to power up, or if it malfunctions, first verify that the power supply is connected correctly. If the problem persists, contact our technical support engineers.

**Caution 2:** Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

### Connection to LINE port

Connect the telephone set to the RJ14 **Phone1/ Phone2 port** for VoIP service.

### Reset Button

In the rear panel, there is a reset button. To load the factory default settings, hold the reset button down for 5 to 10 seconds.

### Connection to ETH port

To connect to a hub or PC, use a RJ45 cable. You can connect the router to up to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

### DSL

Connect to the ADSL port with the ADSL RJ14 cable.

## Chapter 3 Login via Web Browser

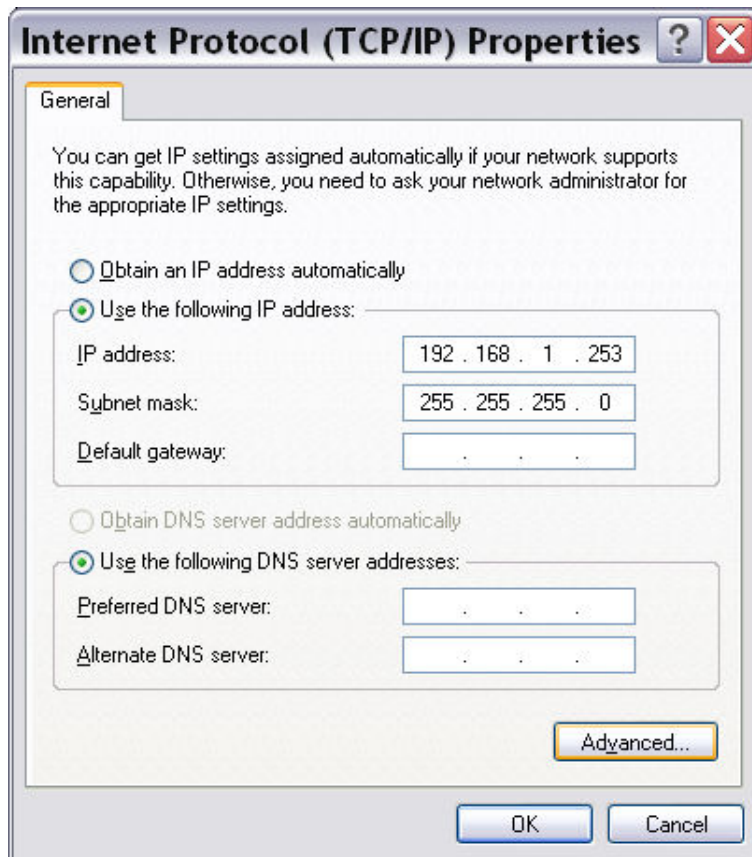
This section describes how to manage the router via a web browser. The web page is best viewed with Microsoft Internet Explorer 5.0 and later. Access Code Required: **#0009@3BFA**. The user can change the Access Code later (see [9.5 Password](#)).

### 3.1 IP Address

The default IP address of the router (LAN port) is 192.168.1.254. To configure the router for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

**STEP 1:** Right click on the Local Area Connection under the Network and Dial-Up connection window and select **Properties**.

**STEP 2:** Enter the TCP/IP window and change the IP address to **192.168.1.x/24**.



**STEP 3:** Click OK to submit settings.


## 3.2 Login Procedure

Perform the following steps to bring up the web browser and configure the router.

**STEP 1:** Start the Internet browser. Type the IP address for the router in the Web address field. For example, if the IP address is 192.168.1.254, type  
`http://192.168.1.254`

# Chapter 4 Device

Select the **Device** button from the main menu to display the **Device Summary** information as here.

at&t Help 

Device | Broadband | Home Network | VOIP | Firewall | Maintenance

Device Summary | Reset Statistics

### Device Summary

**Key Gateway Things to Do**

<a href="#">Troubleshoot</a>	- Perform additional testing
<a href="#">Wireless</a>	- Modify security or settings
<a href="#">Restart your System</a>	- Reboot the gateway
<a href="#">Home Network</a>	- Find a computer, share a file
<a href="#">Gaming and Applications</a>	- Modify your firewall settings
<a href="#">Reset access code</a>	- Forgotten or lost access code

**Modem Information**

Board ID:	96368MBL_1441N
Software Version:	NL-5700-C04_R01
Serial Number:	1065700XXXF-AN000009
Bootloader (CFE) Version:	1.0.37-104.4-10
DSL PHY and Driver Version:	A2pbC030d3.d23b
Wireless Driver Version:	
Date/Time:	Sat Jan 1 00:50:08 2000

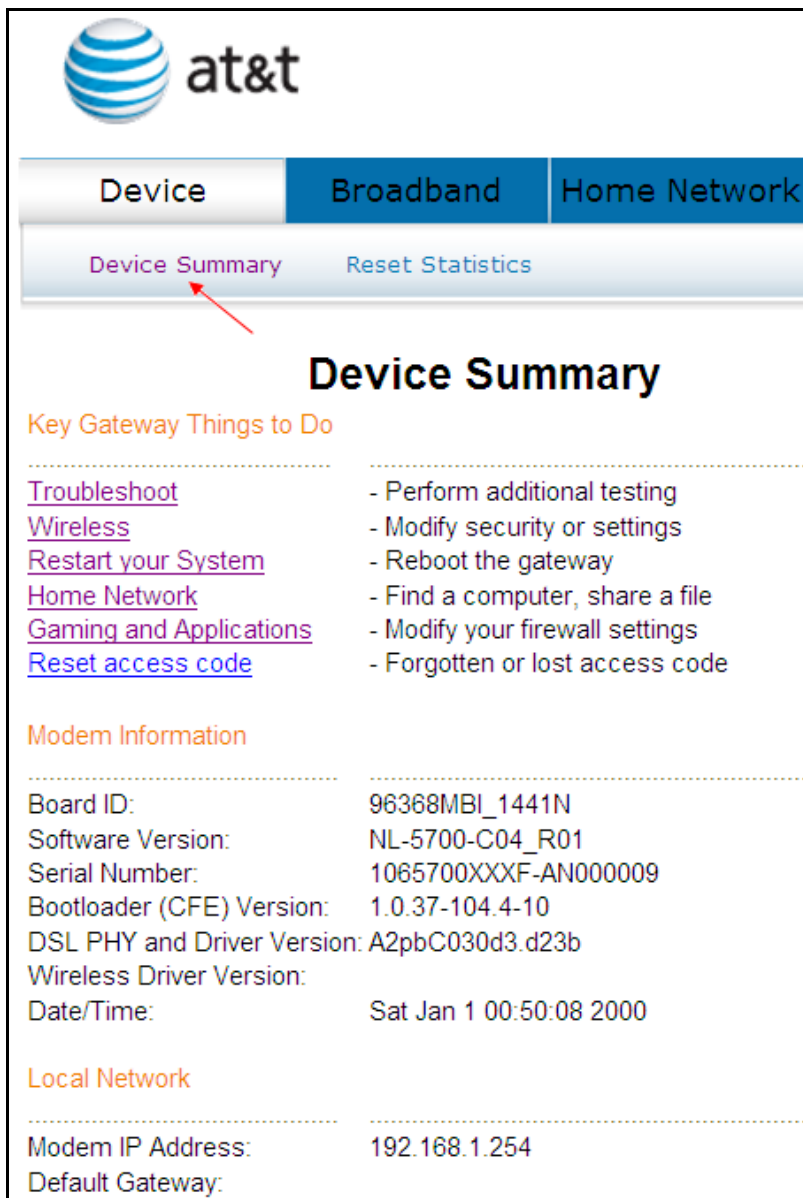
**Local Network**

Modem IP Address:	192.168.1.254
Default Gateway:	

## 4.1 Device Summary

The main menu has several options, and selecting each of these options opens a submenu with more selections.

Subsequent sections will introduce the other main menu options in sequence. The Device Summary screen will display at startup.



**at&t**

Device Broadband Home Network

Device Summary Reset Statistics

### Device Summary

**Key Gateway Things to Do**

<a href="#">Troubleshoot</a>	- Perform additional testing
<a href="#">Wireless</a>	- Modify security or settings
<a href="#">Restart your System</a>	- Reboot the gateway
<a href="#">Home Network</a>	- Find a computer, share a file
<a href="#">Gaming and Applications</a>	- Modify your firewall settings
<a href="#">Reset access code</a>	- Forgotten or lost access code

**Modem Information**

Board ID:	96368MBI_1441N
Software Version:	NL-5700-C04_R01
Serial Number:	1065700XXXF-AN000009
Bootloader (CFE) Version:	1.0.37-104.4-10
DSL PHY and Driver Version:	A2pbC030d3.d23b
Wireless Driver Version:	
Date/Time:	Sat Jan 1 00:50:08 2000

**Local Network**

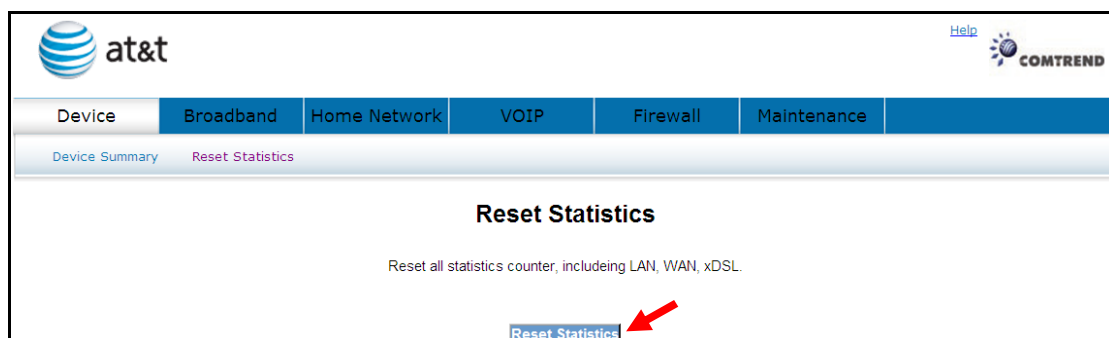
Modem IP Address:	192.168.1.254
Default Gateway:	

## 4.2 Reset Statistics

To reset all statistics including LAN, WAN and xDSL click **Reset Statistics**.



When the following window is displayed, simply click the **Reset Statistics** button to confirm your choice.



## 4.3 Troubleshoot

Your device is capable of testing your DSL connection. Click **Troubleshoot** and the diagnostics window will display.

The screenshot shows the AT&T device management interface. At the top, there is the AT&T logo and a navigation bar with tabs for 'Device', 'Broadband', and 'Home Network'. Below this, there are links for 'Device Summary' and 'Reset Statistics'. The main heading is 'Device Summary'. Underneath, there is a section titled 'Key Gateway Things to Do' which lists several options: 'Troubleshoot', 'Wireless', 'Restart your System', 'Home Network', 'Gaming and Applications', and 'Reset access code'. Each option has a corresponding list of actions. A red arrow points to the 'Troubleshoot' link.

Key Gateway Things to Do	Actions
<a href="#">Troubleshoot</a>	- Perform additional testing
<a href="#">Wireless</a>	- Modify security or settings
<a href="#">Restart your System</a>	- Reboot the gateway
<a href="#">Home Network</a>	- Find a computer, share a file
<a href="#">Gaming and Applications</a>	- Modify your firewall settings
<a href="#">Reset access code</a>	- Forgotten or lost access code

The **Diagnostics** menu provides feedback on the connection status of the device and the ADSL link. Click **Troubleshoot** to bring up the following window.

The screenshot shows the AT&T device management interface with the 'Diagnostics' page. The 'Broadband' tab is selected. The page displays test results for local network and DSL service provider connections. The results are as follows:

Test the connection to your local network		
Test your ENET1 Connection:	FAIL	<a href="#">Help</a>
Test your ENET2 Connection:	FAIL	<a href="#">Help</a>
Test your ENET3 Connection:	FAIL	<a href="#">Help</a>
Test your ENET4 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>
Test the connection to your DSL service provider		
Test xDSL Synchronization:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	DISABLED	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	DISABLED	<a href="#">Help</a>

At the bottom of the page, there are buttons for 'Rerun Diagnostic Tests' and 'Test With OAM F4'.

The individual test results are explained below.

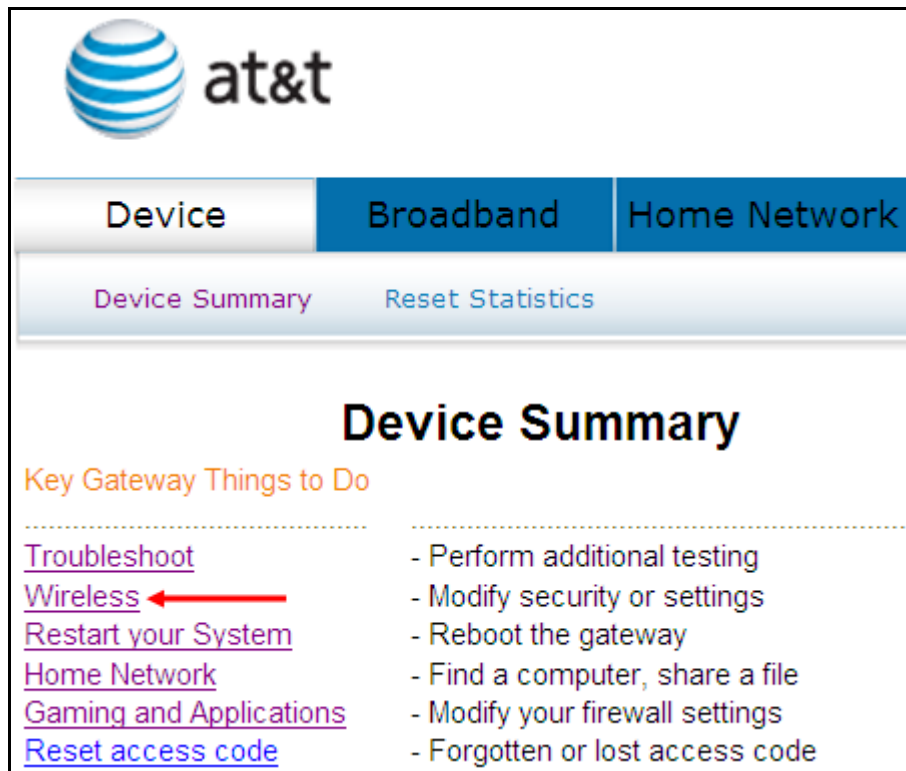


Test	Description
Ethernet Connection	<p><b>Pass:</b> indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful.</p> <p><b>Fail:</b> Indicates that the DSL router does not detect the Ethernet interface on your computer.</p>
Wireless Connection	<p><b>Pass:</b> Indicates that the Wireless interface from your computer is connected to the wireless network.</p> <p><b>Down:</b> Indicates that the DSL router does not detect the wireless network.</p>
DSL Synchronization	<p><b>Pass:</b> Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid WAN LED on the router also indicates the detection of a DSL signal from the telephone company.</p> <p><b>Fail:</b> indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The WAN LED will continue to flash green.</p>

If a test displays a fail status, click the [Rerun Diagnostic Tests](#) button at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures. To test the connection with your DSL service provider, click the [Test With OAM F4](#) button.

## 4.4 Wireless

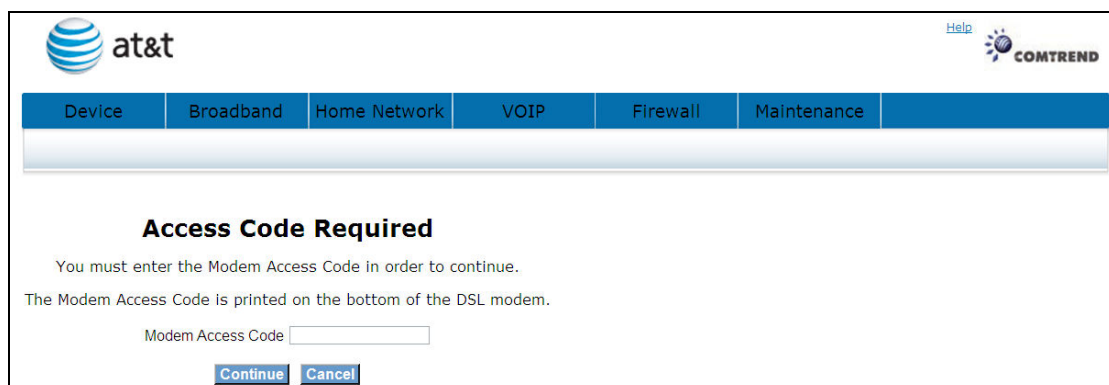
This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



The screenshot shows the AT&T broadband management interface. At the top left is the AT&T logo. Below it is a navigation bar with three tabs: "Device", "Broadband", and "Home Network". The "Broadband" tab is currently selected. Below the navigation bar are two links: "Device Summary" (in purple) and "Reset Statistics" (in blue). The main content area is titled "Device Summary" and contains a section "Key Gateway Things to Do" with a list of links and their corresponding actions:

Link	Action
<a href="#">Troubleshoot</a>	- Perform additional testing
<a href="#">Wireless</a> ←	- Modify security or settings
<a href="#">Restart your System</a>	- Reboot the gateway
<a href="#">Home Network</a>	- Find a computer, share a file
<a href="#">Gaming and Applications</a>	- Modify your firewall settings
<a href="#">Reset access code</a>	- Forgotten or lost access code

Click **Wireless** to bring up the following window.



The screenshot shows a dialog box titled "Access Code Required". At the top left is the AT&T logo, and at the top right is the COMTREND logo. Below the logos is a navigation bar with seven tabs: "Device", "Broadband", "Home Network", "VOIP", "Firewall", and "Maintenance". The "Broadband" tab is selected. The main content area contains the following text:

**Access Code Required**



You must enter the Modem Access Code in order to continue.  
The Modem Access Code is printed on the bottom of the DSL modem.

Modem Access Code

[Continue](#) [Cancel](#)

Input the access code (which is located \_\_\_\_\_) and click the [Continue](#) button.

The options shown here allow you to configure security features of the wireless LAN interface.

[Help](#) 

DeviceBroadbandHome NetworkVOIPFirewallMaintenance

StatusConfigureWireless StatusWireless ConfigureWireless MAC Filter

### Wireless -- Basic Configure

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply Basic Configuration" to configure the basic wireless options.

Enable Wireless

Network Name (SSID):

Wireless -- Security Configure

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually  
OR  
through WiFi Protected Setup(WPS)

WPS Setup

Enable WPS:

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply Security Configuration" when done.

Select SSID:

Network Authentication:

WPA Pre-Shared Key:  [Click here to display](#)

WPA Group Rekey Interval:

WPA Encryption:

WEP Encryption:

Wireless -- Advanced Configure

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply Advanced Configuration" to configure the advanced wireless options.

Channel:  Current: 1

802.11n/EWC:

Bandwidth:

Radio Power Save:

Radio Power Save Quiet Time:

Radio Power Save PPS:

Radio Power Save On Time:

Rate:

Transmit Power:

[Apply Basic Configuration](#)

### 4.4.1 Enable Wireless

<input checked="" type="checkbox"/> Enable Wireless
Network Name (SSID): <input type="text" value="ATT_0009"/>

Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.

### 4.4.2 Wireless - Security Configure

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see [4.4.3 WPS](#)) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID
Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.
Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.

Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	2
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

The settings for WPA authentication are shown below.

Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

The settings for WPA-PSK authentication are shown next.

Network Authentication:	WPA-PSK
WPA Pre-Shared Key:	●●●●●●●●●●●●●●●● <a href="#">Click here to display</a>
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

**WEP Encryption**

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

### **Encryption Strength**

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

### **Current Network Key**

Select the required network key.

### 4.4.3 WPS Setup

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The NexusLink 5700 has both a WPS button on the device and a virtual button accessible from the web user interface (WUI).

Wireless -- Security Configure

This page allows you to configure security features of the wireless LAN interface.  
You may setup configuration manually  
OR  
through WiFi Protected Setup(WPS)

**WPS Setup**

Enable WPS      Disabled ▼

**Manual Setup AP**

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply Security Configuration" when done.

Select SSID:      ATT\_0009 ▼

Network Authentication:      WPA-PSK ▼

WPA Pre-Shared Key:      ●●●●●●●●●● [Click here to display](#)

WPA Group Rekey Interval:      0

WPA Encryption:      AES ▼

WEP Encryption:      Disabled ▼

To configure security settings with WPS, follow the procedures below. You must choose either the Push-Button or PIN configuration method for Steps 6 and 7.

#### I. Setup

**Step 1:** Enable WPS by selecting **Enabled** from the drop down list box shown.

**WPS Setup**

Enable WPS      Enabled ▼

**Step 2:** Set the WPS AP Mode. **Configured** is used when the NexusLink 5700. will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the NexusLink 5700.



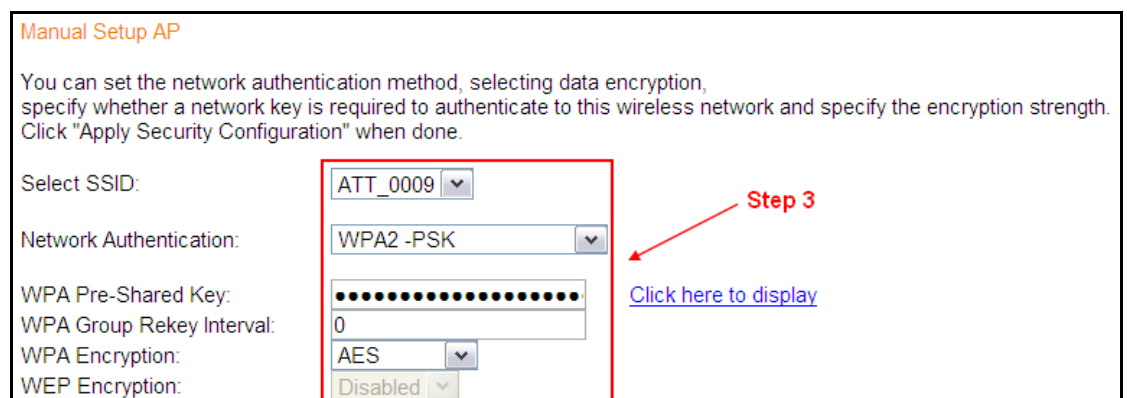
Set WPS AP Mode      Configured ▼

**NOTES:** Your client may or may not have the ability to provide security settings to the NexusLink 5700. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

In addition, using Windows Vista, you can add an external registrar using the **StartAddER** button ([Appendix E - WPS OPERATION](#) has detailed instructions).

## II. NETWORK AUTHENTICATION

**Step 3:** Select Open, WPA-PSK, WPA2-PSK, or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The example below shows WPA2-PSK mode.



Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply Security Configuration" when done.

Select SSID:      ATT\_0009 ▼

Network Authentication:      WPA2 -PSK ▼

WPA Pre-Shared Key:      ●●●●●●●●●●●●●●●●

WPA Group Rekey Interval:      0

WPA Encryption:      AES ▼

WEP Encryption:      Disabled ▼

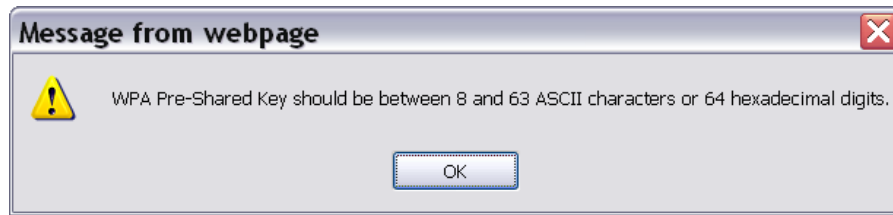
**Step 3**

[Click here to display](#)

**Step 4:** For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key. You



will see the following dialog box if the Key is too short or too long.



**Step 5:** Click the **Apply Basic Configuration** button at the bottom of the window.

### IIIa. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a virtual button (accessible from the web user interface) configuration method.

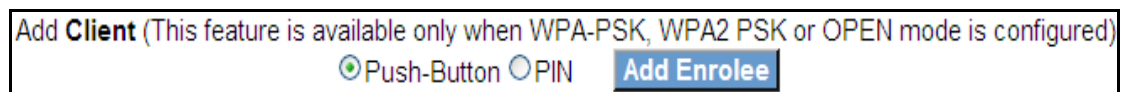
The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

**NOTE:** The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 7, return to Step 6.

#### **Step 6: WUI virtual button**

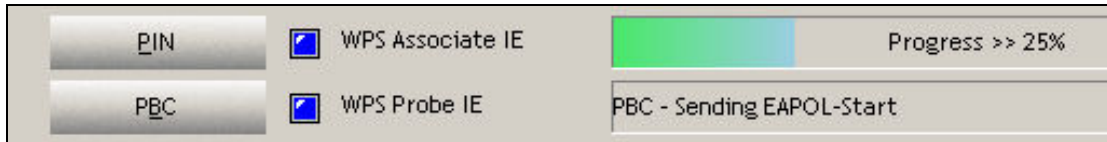
Select the Push-Button radio button in the WPS Setup section of the Wireless Security screen, and then click the appropriate button based on the WPS AP mode selected in step 2.

For **Configured** mode, click the **Add Enrollee** button.



**Step 7:** Go to your WPS wireless client and activate the push-button function on your NexusLink 5700.

A typical WPS client screenshot is shown below as an example.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

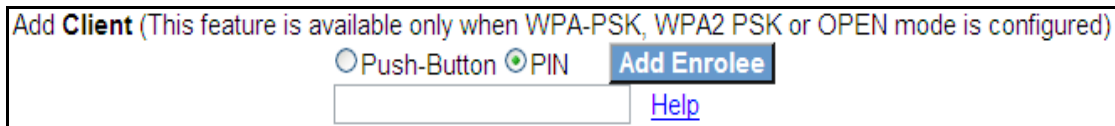
**IIIb. WPS – PIN CONFIGURATION**

Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

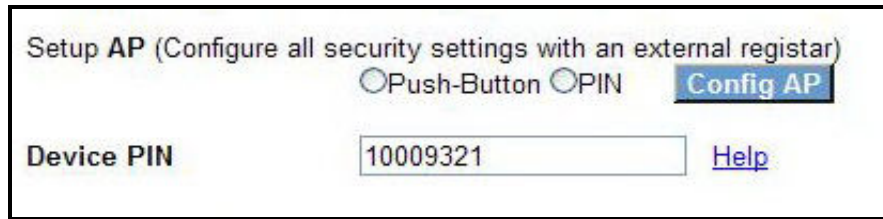
The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

**Step 6:** Select the PIN radio button in the WPS Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WPS AP mode selected in step 2.

**A - For Configured mode,** enter the client PIN in the box provided and then click the **Add Enrollee** button (see below).



**B - For Unconfigured mode,** click the **Config AP** button.



**Step 7:** Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

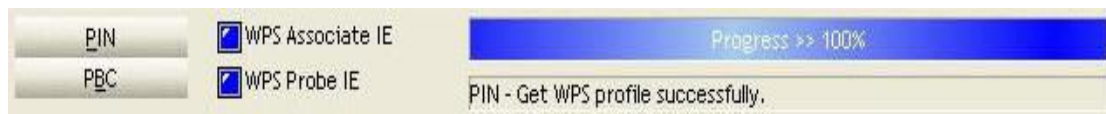
The figure below provides an example of a WPS client PIN function in-progress.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

#### IV. CHECK CONNECTION

**Step 8:** If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

#### 4.4.4 Wireless - Advanced Configure

The Advanced page allows you to configure advanced features of the wireless LAN interface.

You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

**Wireless -- Advanced Configure**

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply Advanced Configuration" to configure the advanced wireless options.

Channel:  Current: 1

802.11n/EWC:

Bandwidth:

Radio Power Save:

Radio Power Save Quiet Time:

Radio Power Save PPS:

Radio Power Save On Time:

Rate:

Transmit Power:

[Apply Basic Configuration](#)

Option	Description
Channel	Drop-down menu that allows selection of a specific channel.
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20MHz or 40MHz bandwidth. 40MHz bandwidth uses two adjacent 20MHz bands for increased data throughput.
Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Transmit Power	Set the power output (by percentage) as desired.

Click the [Apply Basic Configuration](#) button to apply the advanced wireless options.

## **4.5 Restart Your System**

Should you want to reboot the NexusLink 5700, please follow the instructions provided below.

The screenshot shows the AT&T DSL Gateway configuration interface. At the top left is the AT&T logo. Below it is a navigation bar with three tabs: 'Device', 'Broadband', and 'Home Network'. Underneath the navigation bar are two links: 'Device Summary' and 'Reset Statistics'. The main heading is 'Device Summary'. Below this heading is a section titled 'Key Gateway Things to Do'. This section contains a list of links and their corresponding actions:

- [Troubleshoot](#) - Perform additional testing
- [Wireless](#) - Modify security or settings
- [Restart your System](#) ← (indicated by a red arrow) - Reboot the gateway
- [Home Network](#) - Find a computer, share a file
- [Gaming and Applications](#) - Modify your firewall settings
- [Reset access code](#) - Forgotten or lost access code

Click **Restart your System** to bring up the following window.

The screenshot shows the AT&T DSL Gateway configuration interface. At the top left is the AT&T logo. At the top right is the 'Help' link and the COMTREND logo. Below the logo is a navigation bar with six tabs: 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. Underneath the navigation bar are several links: 'Test', 'DSL', 'Ping/Traceroute/NSLooku', 'System Log', 'Password', 'Upgrade', 'Reboot', and 'Factory Reset'. The main heading is 'Diagnostics -- Reboot'. Below this heading is a message: 'Click the button below to reboot the gateway.' and a 'Reboot' button.

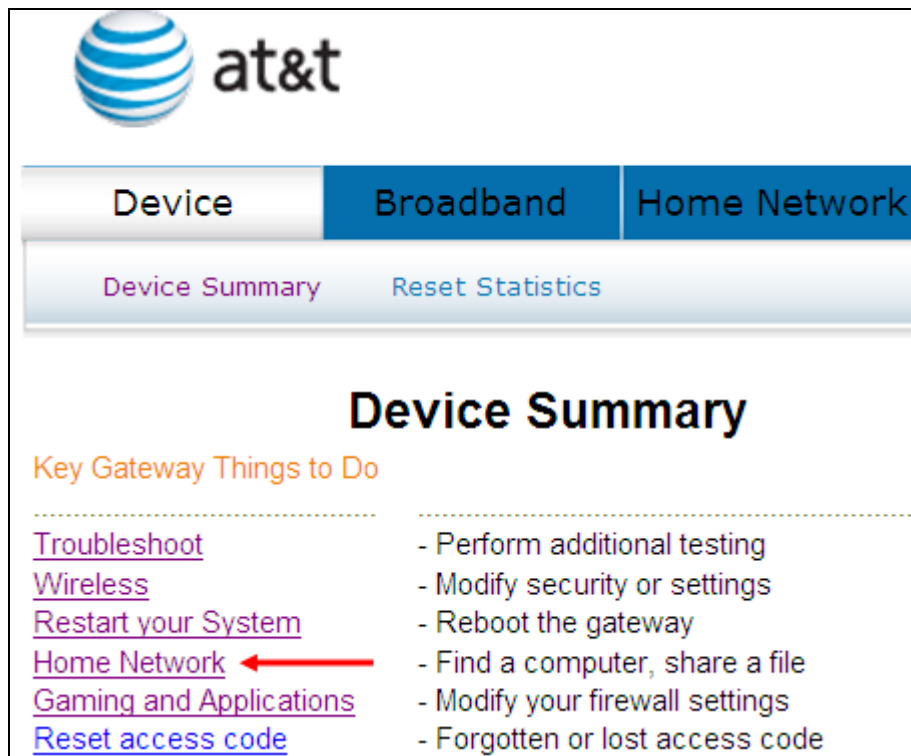
When the following window is displayed, simply click the **Reboot** button to confirm your choice. The following window will display.

**DSL Gateway Reboot**

The DSL Gateway is rebooting.

Close the DSL Gateway Configuration window and wait for 2 minutes before reopening your web browser.

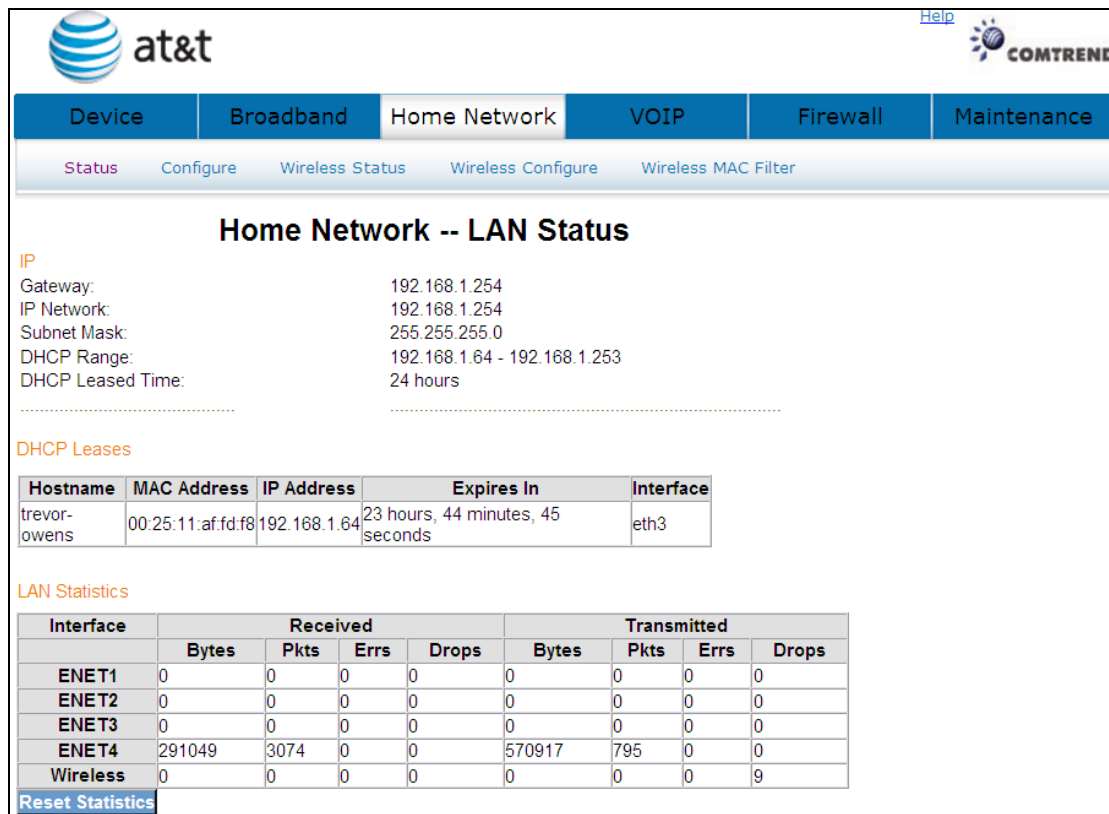
## 4.6 Home Network



The screenshot shows the AT&T Home Network management interface. At the top, there is a navigation bar with tabs for 'Device', 'Broadband', and 'Home Network'. Below this, there are links for 'Device Summary' and 'Reset Statistics'. The main heading is 'Device Summary'. Underneath, there is a section titled 'Key Gateway Things to Do' with a list of links and their corresponding actions:

- [Troubleshoot](#) - Perform additional testing
- [Wireless](#) - Modify security or settings
- [Restart your System](#) - Reboot the gateway
- [Home Network](#) ← Find a computer, share a file
- [Gaming and Applications](#) - Modify your firewall settings
- [Reset access code](#) - Forgotten or lost access code

Click **Home Network** to bring up the following window.



The screenshot shows the AT&T Home Network management interface for LAN Status. The navigation bar includes tabs for 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. Below the navigation bar, there are links for 'Status', 'Configure', 'Wireless Status', 'Wireless Configure', and 'Wireless MAC Filter'. The main heading is 'Home Network -- LAN Status'. The page displays IP configuration details, DHCP Leases, and LAN Statistics.

**IP Configuration:**

- Gateway: 192.168.1.254
- IP Network: 192.168.1.254
- Subnet Mask: 255.255.255.0
- DHCP Range: 192.168.1.64 - 192.168.1.253
- DHCP Leased Time: 24 hours

**DHCP Leases:**

Hostname	MAC Address	IP Address	Expires In	Interface
trevor-owens	00:25:11:af:fd:f8	192.168.1.64	23 hours, 44 minutes, 45 seconds	eth3

**LAN Statistics:**

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ENET1	0	0	0	0	0	0	0	0
ENET2	0	0	0	0	0	0	0	0
ENET3	0	0	0	0	0	0	0	0
ENET4	291049	3074	0	0	570917	795	0	0
Wireless	0	0	0	0	0	0	0	9

At the bottom left, there is a link for 'Reset Statistics'.

Heading	Description
Interface	LAN interface(s)
Received/Transmitted: - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

Click the [Reset Statistics](#) button to refresh this screen.



## 4.7 Gaming and Applications

This window allows you to modify your firewall settings.



at&t

Device Broadband Home Network

Device Summary Reset Statistics

### Device Summary

Key Gateway Things to Do

- [Troubleshoot](#) - Perform additional testing
- [Wireless](#) - Modify security or settings
- [Restart your System](#) - Reboot the gateway
- [Home Network](#) - Find a computer, share a file
- [Gaming and Applications](#) ← - Modify your firewall settings
- [Reset access code](#) - Forgotten or lost access code

Click **Gaming and Applications** to bring up the following window.



Device Broadband Home Network VOIP Firewall Maintenance

Status Inbound Filter Outbound Filter Port Forwarding Port Triggering

### Firewall Status

Firewall setting: On

The gateway is protected by firewall from unfriendly network attacks on the system. To better suit your networking needs, you can configure firewall rules, which grants you additional protections by deny/allow specific traffics to pass through this gateway.

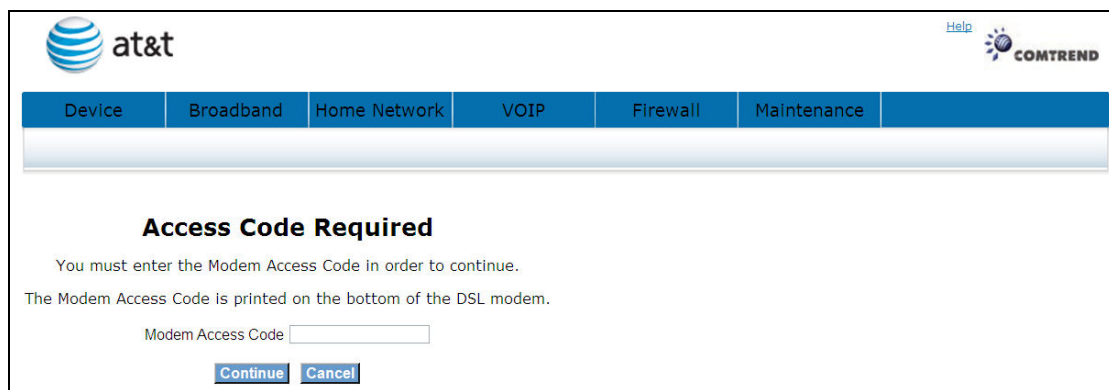
[Incoming Traffic Control](#) [Outgoing Traffic Control](#)

## 4.7.1 Incoming Traffic Control

IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

The default setting for all Incoming traffic is Blocked.

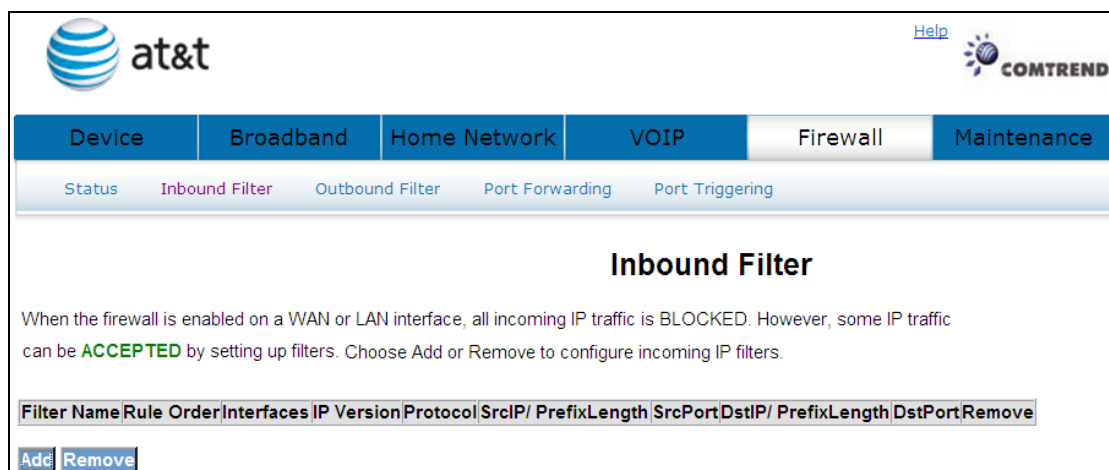
To add or remove IP filters, Click **Incoming Traffic Control**



The screenshot shows the AT&T modem web interface. At the top left is the AT&T logo. At the top right is a 'Help' link and the COMTREND logo. Below the logo is a navigation bar with tabs: Device, Broadband, Home Network, VOIP, Firewall, and Maintenance. The 'Home Network' tab is selected. Below the navigation bar is a message: 'Access Code Required'. The message states: 'You must enter the Modem Access Code in order to continue. The Modem Access Code is printed on the bottom of the DSL modem.' Below the message is a text input field labeled 'Modem Access Code'. At the bottom of the input field are two buttons: 'Continue' and 'Cancel'.

Input the access code (which is located \_\_\_\_\_) and click the **Continue** button.

The options are shown (on the following page)



The screenshot shows the AT&T modem web interface. At the top left is the AT&T logo. At the top right is a 'Help' link and the COMTREND logo. Below the logo is a navigation bar with tabs: Device, Broadband, Home Network, VOIP, Firewall, and Maintenance. The 'Firewall' tab is selected. Below the navigation bar is a sub-navigation bar with tabs: Status, Inbound Filter, Outbound Filter, Port Forwarding, and Port Triggering. The 'Inbound Filter' tab is selected. Below the sub-navigation bar is the title 'Inbound Filter'. Below the title is a paragraph: 'When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters. Choose Add or Remove to configure incoming IP filters.' Below the paragraph is a table with the following columns: Filter Name, Rule, Order, Interfaces, IP Version, Protocol, SrcIP/PrefixLength, SrcPort, DstIP/PrefixLength, DstPort, and Remove. Below the table are two buttons: 'Add' and 'Remove'.

To add a filtering rule, click the **Add** button. The following window will be displayed.

The screenshot shows the AT&T Comtrend web interface. At the top, there are logos for AT&T and Comtrend, along with a 'Help' link. Below the logos is a navigation menu with tabs for 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. Under the 'Firewall' tab, there are sub-tabs for 'Status', 'Inbound Filter', 'Outbound Filter', 'Port Forwarding', and 'Port Triggering'. The main heading is 'Add IP Filter -- Incoming'. Below this, there is a paragraph explaining that the screen allows creating a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. It states that all specified conditions must be satisfied for the rule to take effect and that the user should click 'Apply/Save' to save and activate the filter.

The form fields are as follows:

- Filter Name:
- Rule Order:
- IP Version:
- Protocol:
- Source IP address[/prefix length]:
- Source Port (port or port:port):
- Destination IP address[/prefix length]:
- Destination Port (port or port:port):

Below the form, there is a note: 'WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces'. A sub-heading reads: 'Select one or more WAN/LAN interfaces displayed below to apply this rule.' There are three checkboxes with labels: 'Select All', 'ipoe\_0\_1\_1.0/ptm0.0', and 'br0/br0'. At the bottom left of the form area is an 'Apply/Save' button.

Filter Name	Type a name for the filter rule.
Rule Order	Execute IP Filter order. (Available in future versions).
IP Version	IPv4 selected by default.
Protocol	User can select: TCP, TCP/UDP, UDP or ICMP.
Source IP address	Input source IP address.
Source Subnet Mask	Input source subnet mask.
Source Port (port or port:port)	Input source port number.
Destination IP address	Input destination IP address.
Destination Subnet Mask	Input destination subnet mask.
Destination port (port or port:port)	Input destination port number.

Click **Apply/Save** to save and activate the filter.

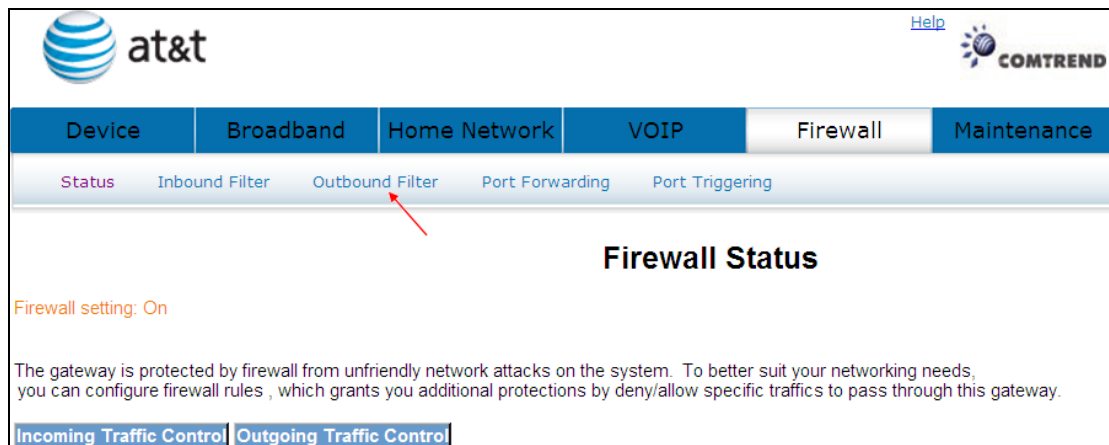
Click **Remove** to delete a filter.

## 4.7.2 Outgoing Traffic Control

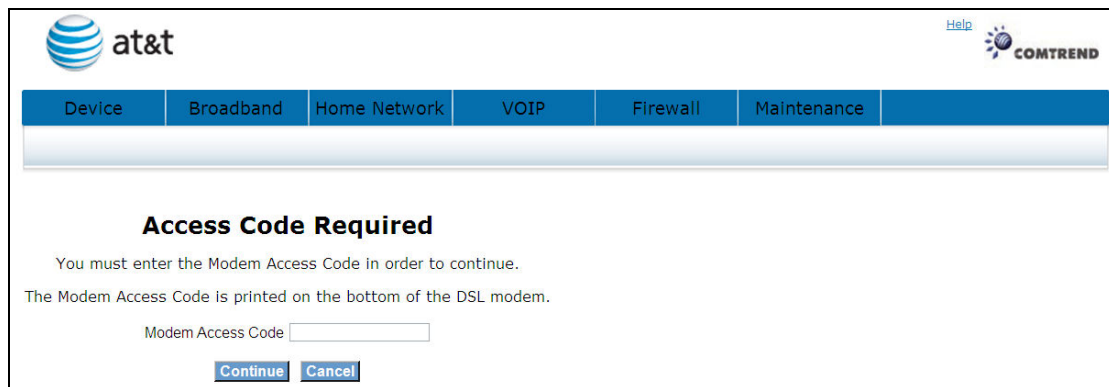
IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

The default setting for all Outgoing traffic is Accepted.

To add or remove IP filters, Click **Outgoing Traffic Control**



The screenshot shows the AT&T modem web interface. At the top left is the AT&T logo, and at the top right is the COMTREND logo with a "Help" link. Below the logos is a navigation bar with tabs: Device, Broadband, Home Network, VOIP, Firewall, and Maintenance. Under the Firewall tab, there are sub-tabs: Status, Inbound Filter, Outbound Filter, Port Forwarding, and Port Triggering. A red arrow points to the "Outbound Filter" sub-tab. The main content area is titled "Firewall Status" and displays "Firewall setting: On". Below this, there is a paragraph explaining that the gateway is protected by a firewall and that users can configure firewall rules. At the bottom of the content area, there are two buttons: "Incoming Traffic Control" and "Outgoing Traffic Control".



The screenshot shows the AT&T modem web interface with an "Access Code Required" message. The navigation bar is the same as in the previous screenshot. The main content area is titled "Access Code Required" and contains the text: "You must enter the Modem Access Code in order to continue. The Modem Access Code is printed on the bottom of the DSL modem." Below this text is a text input field labeled "Modem Access Code". At the bottom of the input field are two buttons: "Continue" and "Cancel".

Input the access code (which is located \_\_\_\_\_) and click the **Continue** button.

The options are shown (on the following page)

To add a filtering rule, click the **Add** button. The following window will be displayed.

Filter Name	Type a name for the filter rule.
Rule Order	Execute IP Filter order. (Available in future versions).
IP Version	IPv4 selected by default.
Protocol	User can select: TCP, TCP/UDP, UDP or ICMP.
Source IP address	Input source IP address.
Source Subnet Mask	Input source subnet mask.
Source Port (port or port:port)	Input source port number.
Destination IP address	Input destination IP address.
Destination Subnet Mask	Input destination subnet mask.
Destination port (port or port:port)	Input destination port number.

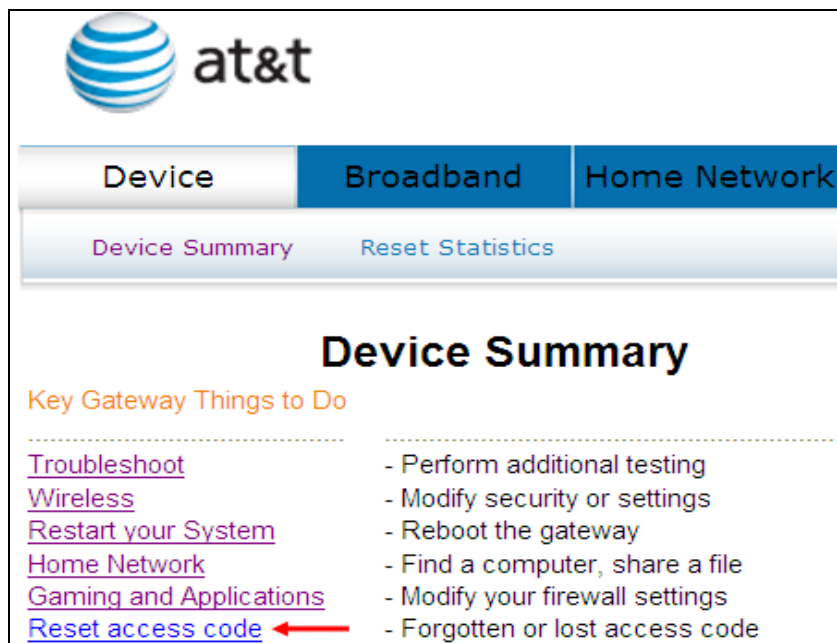
Click **Apply/Save** to save and activate the filter.

Click **Remove** to delete a filter.

## 4.8 Reset Access Code

To help prevent unauthorized access to your router, be sure you record your Modem Access Code and safeguard it just as you would any other password or PIN number. Should you need access to your router (for example, to make configuration changes or to change your Internet Service Provider login password) you will need the modem access code.

**Note: This modem access code is separate from the password that you use to log in to your Internet Service Provider, and it is strongly recommend you use a different value for your access code for security reasons.**



at&t

Device Broadband Home Network

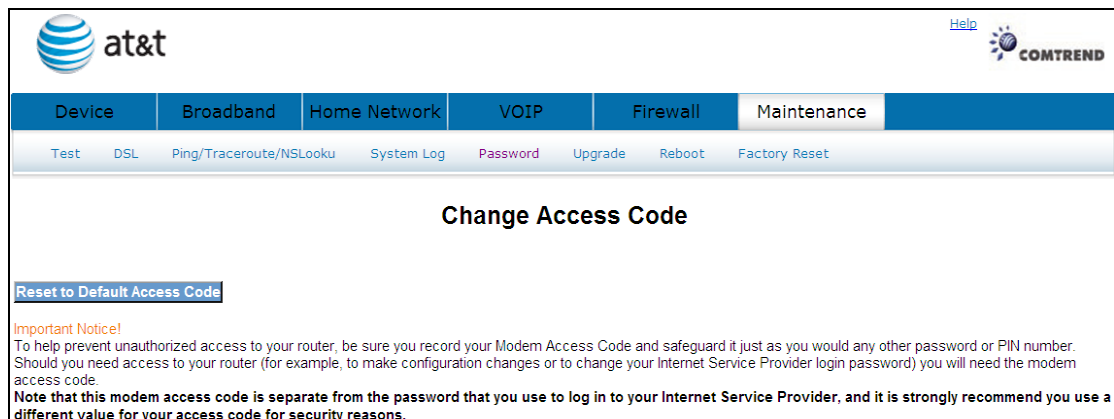
Device Summary Reset Statistics

### Device Summary

Key Gateway Things to Do

- [Troubleshoot](#) - Perform additional testing
- [Wireless](#) - Modify security or settings
- [Restart your System](#) - Reboot the gateway
- [Home Network](#) - Find a computer, share a file
- [Gaming and Applications](#) - Modify your firewall settings
- [Reset access code](#) ← - Forgotten or lost access code

Click **Reset access code** to bring up the following window.



at&t

Help COMTREND

Device Broadband Home Network VOIP Firewall Maintenance

Test DSL Ping/Traceroute/NSLookup System Log Password Upgrade Reboot Factory Reset

### Change Access Code

[Reset to Default Access Code](#)

**Important Notice!**  
To help prevent unauthorized access to your router, be sure you record your Modem Access Code and safeguard it just as you would any other password or PIN number. Should you need access to your router (for example, to make configuration changes or to change your Internet Service Provider login password) you will need the modem access code.  
**Note that this modem access code is separate from the password that you use to log in to your Internet Service Provider, and it is strongly recommend you use a different value for your access code for security reasons.**

If you have lost or forgotten your new access code, click

**Reset to Default Access Code** to se to default.

# Chapter 5 Broadband

This window shows the existing WAN status.

## 5.1 Status

Click **Broadband** to display the status of all configured PVC(s).

**Broadband -- WAN Status**

**DSL Connection Details**  
 Bonding: PTM  
 Line Rate - Downstream: 0 Kbps  
 Line Rate - Upstream: 0 Kbps

**Internet Connection Details**

<b>Internet Address:</b>	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0

**WAN Statistics**

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ptm0.0	ipoe_0_1_1.0	0	0	0	0	0	0	0	0

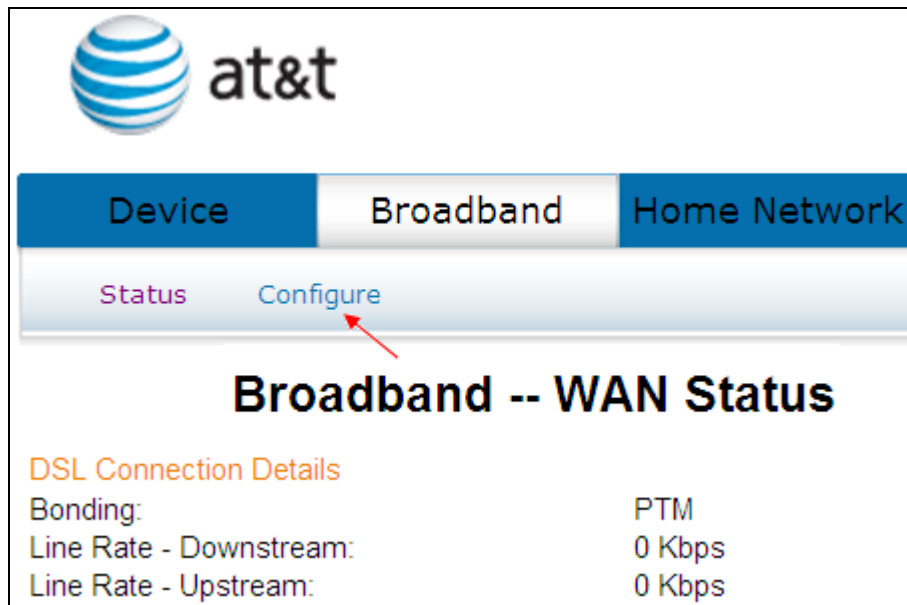
[Reset Statistics](#)

Port/VPI/VCI	Shows the values of the ATM Port/VPI/VCI
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the statue of the IGMP function
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows IP address for WAN interface

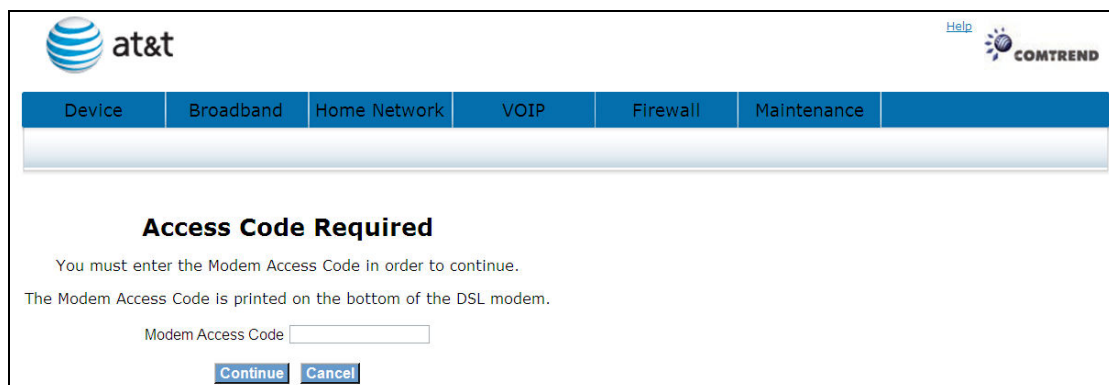
Click [Reset Statistics](#) to reset the status of all configured PVC(s).



## 5.2 Configure



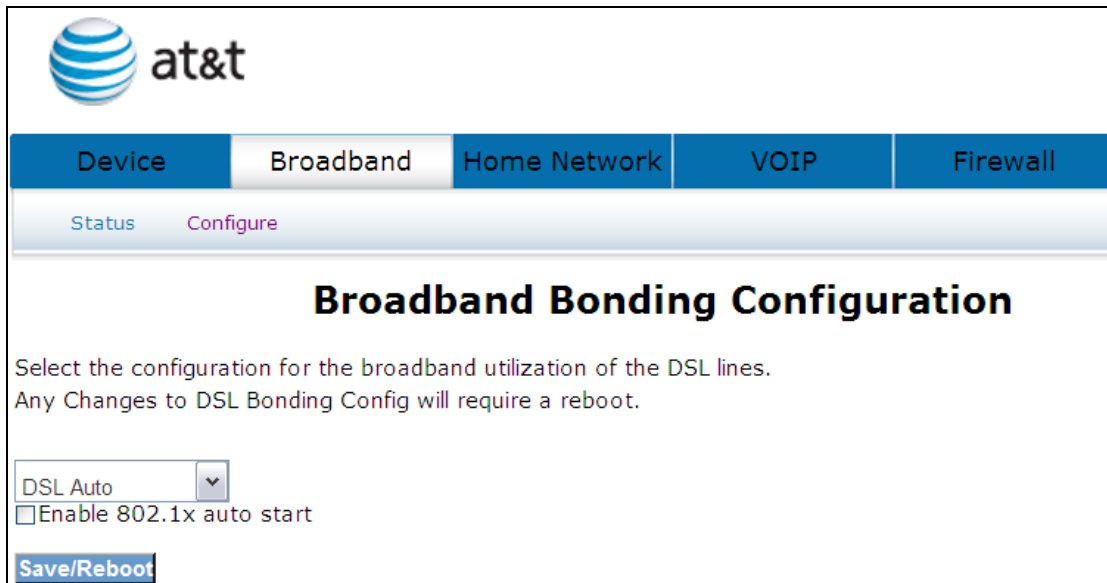
Click **Configure** will bring up the following window.



Input the access code (which is located \_\_\_\_\_) and click the **Continue** button.

The options are shown (on the following page)

Select the configuration for the broadband utilization of the DSL lines. Any Changes to DSL Bonding Config will require a reboot.



The screenshot shows the AT&T web interface for broadband configuration. At the top left is the AT&T logo. Below it is a navigation bar with tabs for 'Device', 'Broadband', 'Home Network', 'VOIP', and 'Firewall'. Under the 'Broadband' tab, there are two sub-links: 'Status' and 'Configure'. The main heading is 'Broadband Bonding Configuration'. Below the heading, there is a paragraph of text: 'Select the configuration for the broadband utilization of the DSL lines. Any Changes to DSL Bonding Config will require a reboot.' Below this text is a dropdown menu currently set to 'DSL Auto' with a downward arrow. Underneath the dropdown is a checkbox labeled 'Enable 802.1x auto start'. At the bottom left of the configuration area is a blue button labeled 'Save/Reboot'.

Select one of the three options (DSL Auto, DSL on inner pair, DSL on outer pair) from the drop down menu and tick the Enable 802.1x auto start box if required. Click the **Save/Reboot** button to confirm your choice(s).

# Chapter 6 Home Network

The Home Network – LAN Status screen shows interface statistics for Ethernet and Wireless interfaces.

## 6.1 LAN Status

The Network Statistics screen shows interface statistics for LAN of Ethernet interface. Here provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)

The screenshot shows the 'Home Network -- LAN Status' page. At the top, there are logos for 'at&t' and 'COMTREND'. Below the logos is a navigation bar with tabs: 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. Underneath the navigation bar are links: 'Status', 'Configure', 'Wireless Status', 'Wireless Configure', and 'Wireless MAC Filter'. The main content area is titled 'Home Network -- LAN Status' and contains the following sections:

**IP**  
Gateway: 192.168.1.254  
IP Network: 192.168.1.254  
Subnet Mask: 255.255.255.0  
DHCP Range: 192.168.1.64 - 192.168.1.253  
DHCP Leased Time: 24 hours

**DHCP Leases**

Hostname	MAC Address	IP Address	Expires In	Interface
	00:25:11:af:fd:f8	192.168.1.64	23 hours, 16 minutes, 5 seconds	eth3

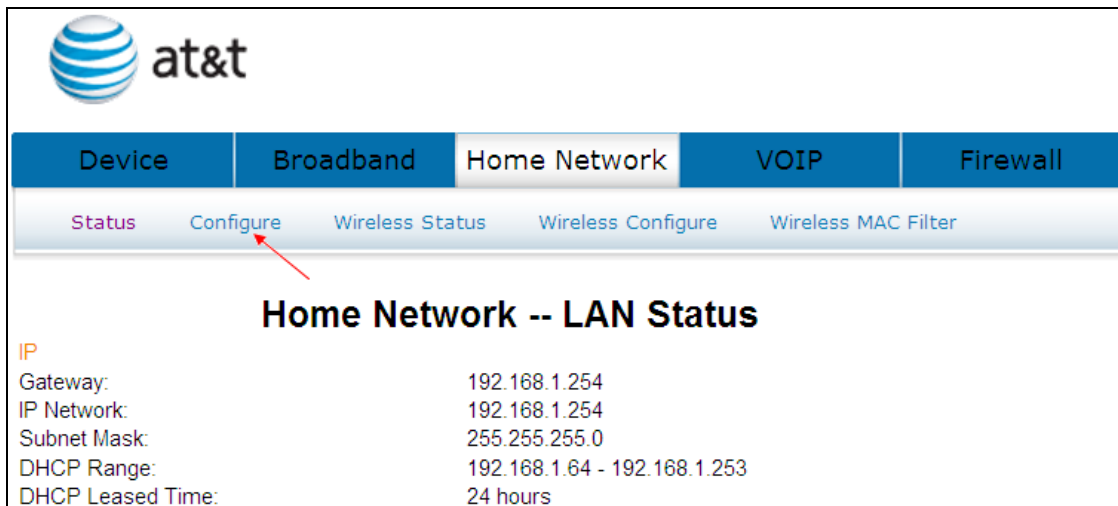
**LAN Statistics**

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ENET1	0	0	0	0	0	0	0	0
ENET2	0	0	0	0	0	0	0	0
ENET3	0	0	0	0	0	0	0	0
ENET4	1941466	21065	0	0	3039484	4272	0	0
Wireless	19	1	0	0	0	31	1	15

At the bottom left of the statistics table, there is a button labeled 'Reset Statistics'.

Click the **Reset Statistics** button to refresh this screen.

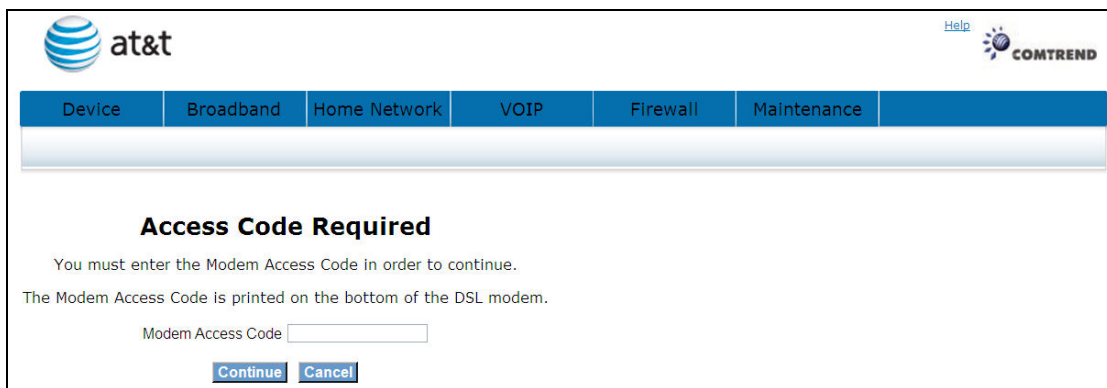
## 6.2 Configure



The screenshot shows the AT&T modem configuration interface. At the top left is the AT&T logo. Below it is a navigation bar with tabs for Device, Broadband, Home Network, VOIP, and Firewall. Under the Home Network tab, there are sub-tabs: Status, Configure, Wireless Status, Wireless Configure, and Wireless MAC Filter. A red arrow points to the 'Configure' sub-tab. Below the navigation bar, the page title is 'Home Network -- LAN Status'. Underneath, there is a table of network information:

IP	
Gateway:	192.168.1.254
IP Network:	192.168.1.254
Subnet Mask:	255.255.255.0
DHCP Range:	192.168.1.64 - 192.168.1.253
DHCP Leased Time:	24 hours

Click **Configure** to bring up the following window.



The screenshot shows the AT&T modem configuration interface. At the top left is the AT&T logo. At the top right is a 'Help' link and the COMTREND logo. Below the logo is a navigation bar with tabs for Device, Broadband, Home Network, VOIP, Firewall, and Maintenance. Below the navigation bar, the page title is 'Access Code Required'. Below the title, there is a message: 'You must enter the Modem Access Code in order to continue. The Modem Access Code is printed on the bottom of the DSL modem.' Below the message, there is a text input field labeled 'Modem Access Code'. Below the input field, there are two buttons: 'Continue' and 'Cancel'.

Input the access code (which is located \_\_\_\_\_) and click the **Continue** button.

The options are shown (on the following page)

at&t Help

Device | **Broadband** | Home Network | VOIP | Firewall | Maintenance

Status | **Configure** | Wireless Status | Wireless Configure | Wireless MAC Filter

### Home Network Configure -- LAN Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:   
 Subnet Mask:

Disable DHCP Server  
 Enable DHCP Server

Start IP Address:   
 End IP Address:   
 Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove Entries"/>

#### Additional Subnet Configuration

Define additional lan subnets.

Group Name	IP Address	Subnet Mask	Remove
Default			<input type="button" value="Remove Subnet"/>

Configure the second IP Address and Subnet Mask for LAN interface

#### Ethernet Media Type

Port 1    
 Port 2    
 Port 3    
 Port 4

Configure the DSL router IP address and subnet mask for the LAN interface.

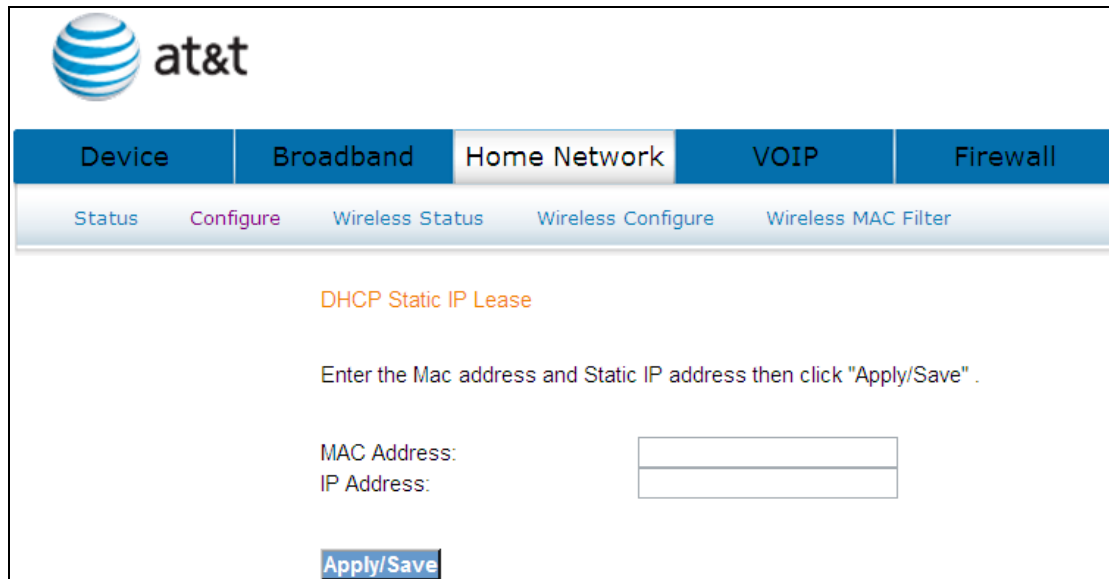
**IP ADDRESS:** ENTER THE IP ADDRESS FOR THE LAN PORT.

**SUBNET MASK:** ENTER THE SUBNET MASK FOR THE LAN PORT.

**DHCP Server:** To enable DHCP, select **Enable DHCP server** and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

**Static IP Lease List:** A maximum of 32 entries can be configured.

Click **Add Entries** to add a DHCP static IP lease. The following window will be displayed.



The screenshot shows the AT&T Home Network configuration interface. At the top left is the AT&T logo. Below it is a navigation bar with tabs for Device, Broadband, Home Network (selected), VOIP, and Firewall. Under the Home Network tab, there are sub-tabs for Status, Configure (selected), Wireless Status, Wireless Configure, and Wireless MAC Filter. The main content area is titled "DHCP Static IP Lease" and contains the instruction: "Enter the Mac address and Static IP address then click 'Apply/Save'". Below this instruction are two input fields: "MAC Address:" and "IP Address:". At the bottom of the form is an "Apply/Save" button.

Input the MAC address and Static IP address and then click **Apply/Save**

To remove an entry, tick the corresponding checkbox  in the Remove column and then click the **Remove Entries** button.

Click **Add New Subnet** to input the secondary subnet mask for the LAN port.

**Lan Subnet Configuration**

To create a new subnet group for LAN Devices:

1. Enter the Group name and the group name must be unique
2. Select the intended application of the new subnet group
3. Enter the corresponding IP and DHCP address
4. Passthrough MAC Address only needs to be entered in passthrough mode for the specific device that needs to share the WAN IP address
5. You can define the IP address of the router device within the subnet in Route To LAN IP Address for automatic routing rules to direct traffics to it; If the routing requires a different subnet set, you can define it in Routing Subnet
6. If Secondary IP Address is empty, it will be calculated as one address less than the last address of the defined subnet for the dhcp server.

**Note:** For Passthrough mode to correctly route the traffic, you need to reboot the gateway

Group Name:

Use Allocated WAN:  Normal - NAT

Bypass Firewall Protection:

Secondary IP Address:

Subnet Mask:

DHCP Start IP Address:

DHCP End IP Address:

Leased Time (second):

Passthrough MAC Address:

Route To LAN IP Address:

Route To LAN Subnet:

WAN Interface used in the grouping:

Grouped LAN Interfaces:

Available LAN Interfaces: ENET1, ENET2, ENET3, ENET4, wlan0

To create a new subnet group for LAN Devices:

1. Enter the Group name and the group name must be unique
2. Select the intended application of the new subnet group
3. Enter the corresponding IP and DHCP address
4. Passthrough MAC Address only needs to be entered in passthrough mode for the specific device that needs to share the WAN IP address
5. You can define the IP address of the router device within the subnet in Route To LAN IP Address for automatic routing rules to direct traffics to it; If the routing requires a different subnet set, you can define it in Routing Subnet
6. If Secondary IP Address is empty, it will be calculated as one address less than the last address of the defined subnet for the dhcp server.

**Note:** For Passthrough mode to correctly route the traffic, you need to reboot the gateway

## **2<sup>ND</sup> LAN INTERFACE**

To configure a secondary IP address, tick the checkbox  as shown here.

<input checked="" type="checkbox"/>	Configure the second IP Address and Subnet Mask for LAN interface
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

**IP Address:** Enter the secondary IP address for the LAN port.

**Subnet Mask:** Enter the secondary subnet mask for the LAN port.

Click **Apply/Save** to confirm.

Ethernet Media Type: Each LAN port has Speed/Duplex Negotiation detection capability, the LAN ports detect the speed (for example, 10MBps, 100Mbps) and duplex (half-duplex or full-duplex) settings of the device on the other end of the wire and subsequently adjusts to match those settings. During speed/duplex negotiation the device transmits its own abilities to the peer device so that the peer can use the appropriate settings.

Auto: Auto detects Speed/Duplex Negotiation

**10\_Half:** The speed limit is 10M and Duplex Negotiation is half.

**10\_Full:** The speed limit is 100M and Duplex Negotiation is full.

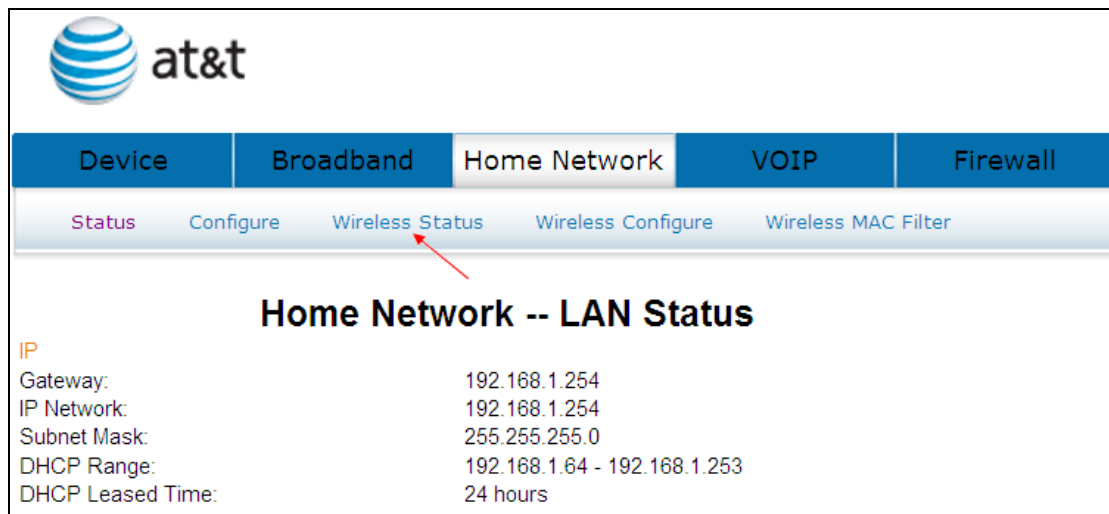
**100\_Half:** The speed limit is 100M and Duplex Negotiation is half.

**100\_Full:** The speed limit is 100M and Duplex Negotiation is full.

Ethernet Media Type		
Port 1	Auto	▼
Port 2	Auto	▼
Port 3	Auto	▼
Port 4	Auto	▼



## 6.3 Wireless Status



The screenshot shows the AT&T router configuration interface. The top navigation bar includes tabs for Device, Broadband, Home Network, VOIP, and Firewall. Below this, a secondary navigation bar has links for Status, Configure, Wireless Status, Wireless Configure, and Wireless MAC Filter. A red arrow points to the 'Wireless Status' link. The main content area is titled 'Home Network -- LAN Status' and displays the following network information:

IP	
Gateway:	192.168.1.254
IP Network:	192.168.1.254
Subnet Mask:	255.255.255.0
DHCP Range:	192.168.1.64 - 192.168.1.253
DHCP Leased Time:	24 hours

Click **Wireless Status** to bring up the following window.



The screenshot shows the AT&T router configuration interface with the 'Wireless Status' page selected. The top navigation bar includes tabs for Device, Broadband, Home Network, VOIP, Firewall, and Maintenance. Below this, a secondary navigation bar has links for Status, Configure, Wireless Status, Wireless Configure, and Wireless MAC Filter. The main content area is titled 'Wireless Status -- Authenticated Stations' and includes the following text and elements:

This page shows authenticated wireless stations and their status.

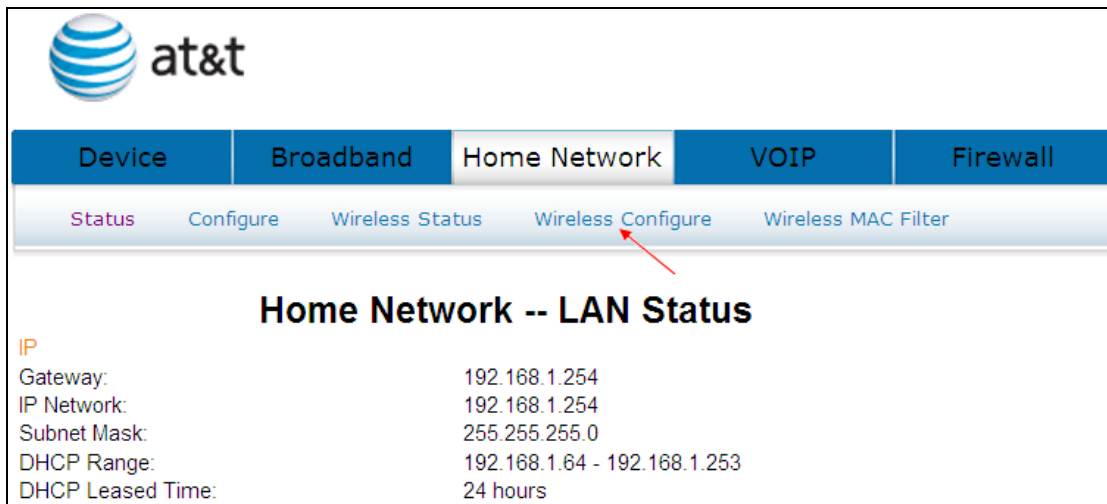
MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

[Refresh](#)

Click [Refresh](#) to reset the screen.

## 6.4 Wireless Configure

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



The screenshot shows the AT&T router configuration interface. At the top left is the AT&T logo. Below it is a navigation bar with five tabs: 'Device', 'Broadband', 'Home Network', 'VOIP', and 'Firewall'. Under the 'Home Network' tab, there are five sub-links: 'Status', 'Configure', 'Wireless Status', 'Wireless Configure', and 'Wireless MAC Filter'. A red arrow points to the 'Wireless Configure' link. Below the navigation bar, the page title is 'Home Network -- LAN Status'. To the left of this title, the word 'IP' is written in orange. Below the title, there is a table of network settings:

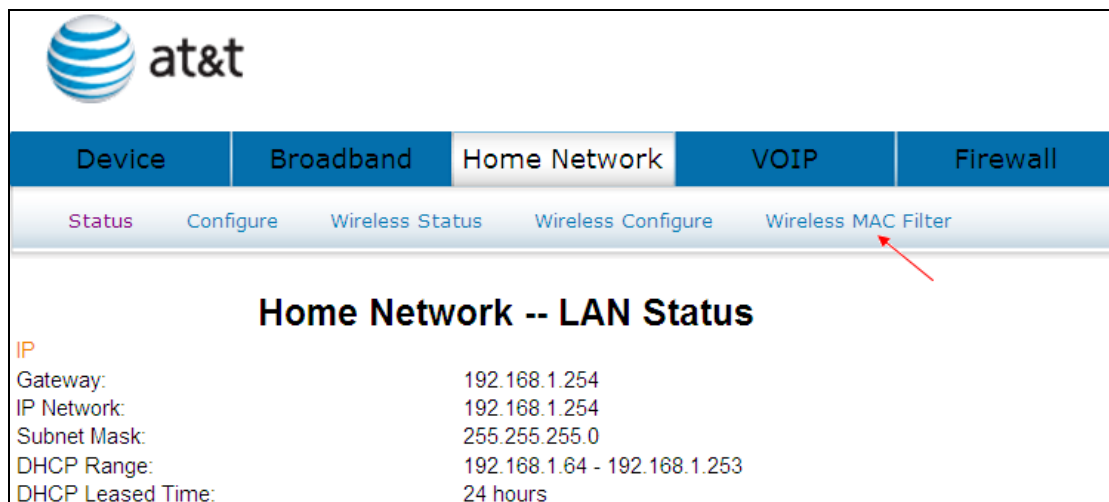
Gateway:	192.168.1.254
IP Network:	192.168.1.254
Subnet Mask:	255.255.255.0
DHCP Range:	192.168.1.64 - 192.168.1.253
DHCP Leased Time:	24 hours

See section: [4.4 Wireless](#) for a detailed description.

## 6.5 Wireless MAC Filter

When a device is using MAC filtering, any address not explicitly defined will be denied access.

This MAC Filter page allows access to be restricted/allowed based on a MAC address. All (Network Interface Cards) NICs have a unique 48-bit MAC address burned into the ROM chip on the card. When MAC address filtering is enabled, you are restricting the NICs that are allowed to connect to your access point. Therefore, an access point will grant access to any computer that is using a NIC whose MAC address is on its "allows" list.



at&t

Device Broadband Home Network VOIP Firewall

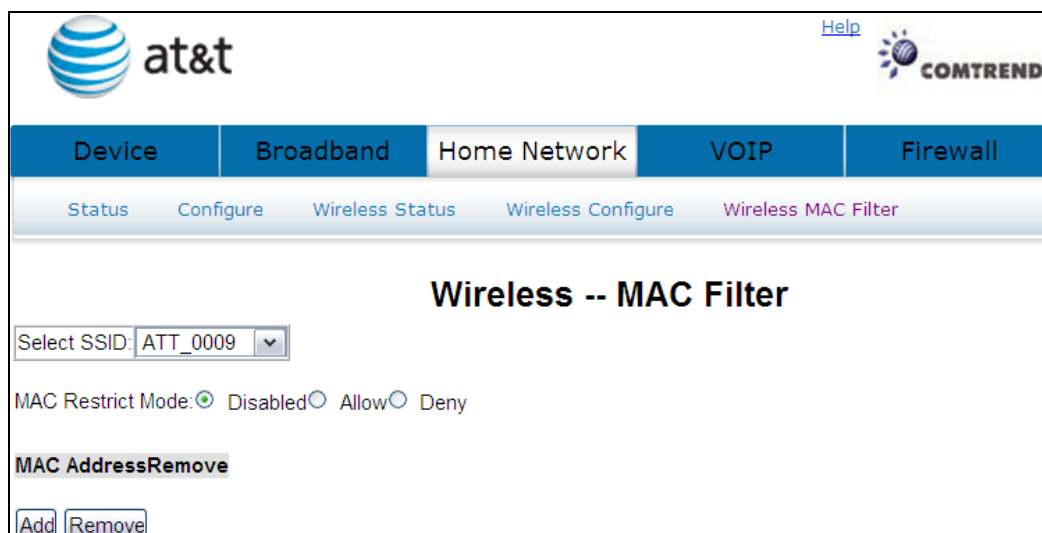
Status Configure Wireless Status Wireless Configure Wireless MAC Filter

### Home Network -- LAN Status

IP

Gateway:	192.168.1.254
IP Network:	192.168.1.254
Subnet Mask:	255.255.255.0
DHCP Range:	192.168.1.64 - 192.168.1.253
DHCP Leased Time:	24 hours

Click **Wireless MAC Filter** to bring up the following window.



at&t

Help COMTREND

Device Broadband Home Network VOIP Firewall

Status Configure Wireless Status Wireless Configure Wireless MAC Filter

### Wireless -- MAC Filter

Select SSID: ATT\_0009

MAC Restrict Mode:  Disabled  Allow  Deny

**MAC AddressRemove**

Add Remove

MAC Restrict mode: **Off**- disables MAC filtering; **Allow** – permits **access** for the specified MAC address; **deny**; reject access of the specified MAC address, then click the **SET** button.

Option	Description
MAC Restrict Mode	Radio buttons that allow settings of; Off: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the Off, Allow, or Deny instruction. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. The maximum number of MAC addresses that can be added is 60.

To add a MAC entry, click **Add** and input a MAC address

The screenshot shows the AT&T web interface for configuring wireless settings. The top navigation bar includes 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. Under 'Home Network', there are links for 'Status', 'Configure', 'Wireless Status', 'Wireless Configure', and 'Wireless MAC Filter'. The 'Wireless MAC Filter' page is displayed, featuring the title 'Wireless -- MAC Filter' and the instruction: 'Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.' Below this is a text input field labeled 'MAC Address:' and an 'Apply/Save' button.

Click **Apply/Save** to add the MAC address to the wireless MAC address filters. To

delete an entry, select the entry, click the **Remove** button.

## Chapter 7 VOIP

This chapter first describes the various options for configuration of the SIP voice service. It then provides detailed instructions for making telephone calls using VoIP (Voice over IP) or PSTN (Public Switched Telephone Network)<sup>(1)</sup> services.

Session Initiation Protocol (SIP) is a peer-to-peer protocol used for Internet conferencing, telephony, events notification, presence and instant messaging. SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

(1) The NexusLink 5700 supports Phone Line (FXS) interface only, which cannot dial to the local PSTN network.

**NOTE:** The SIP standard is set by the Internet Engineering Task Force (IETF).

The SIP standard defines the following agents/servers:

User Agents (**UA**) - SIP phone clients (hardware or software)

Proxy Server – relays data between **UA** and external servers

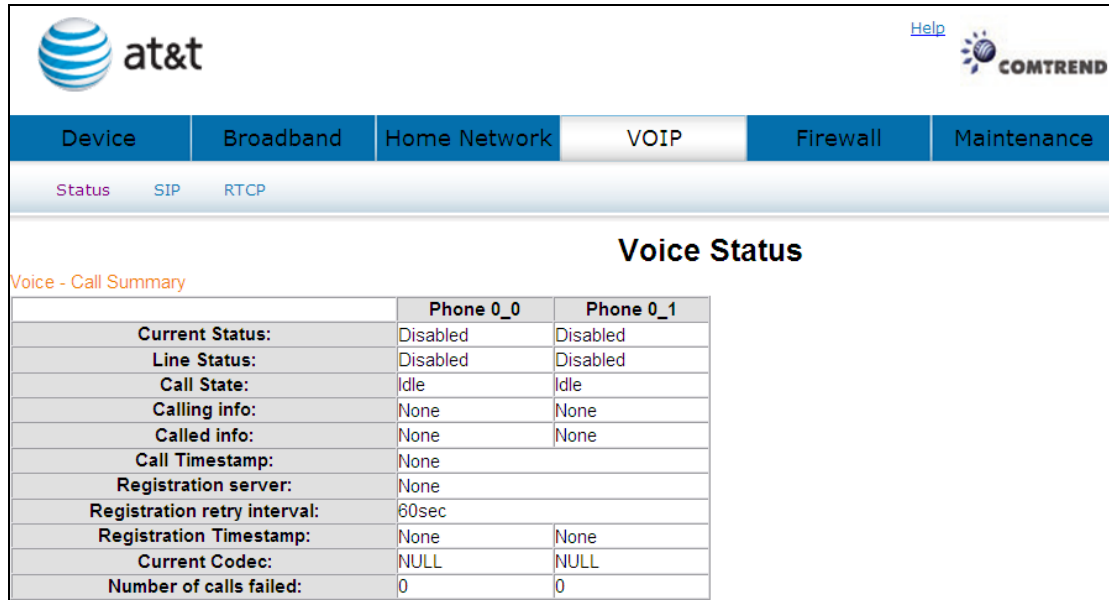
Registrar Server - a server that accepts register requests from **UA**

Redirect Server – provides an address lookup service to **UA**

---

## 7.1 Status

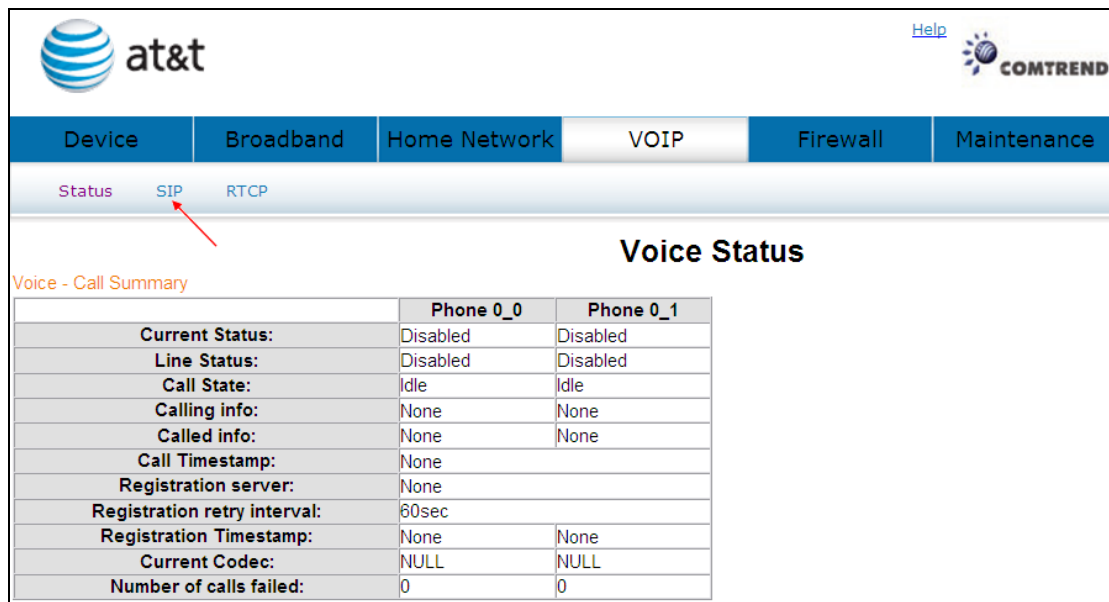
Displays the call summary.



The screenshot shows the AT&T Comtrend web interface. The top navigation bar includes 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. The 'Status' tab is selected, and the 'Voice Status' page is displayed. The 'Voice - Call Summary' table is shown below the navigation bar.

	Phone 0_0	Phone 0_1
Current Status:	Disabled	Disabled
Line Status:	Disabled	Disabled
Call State:	Idle	Idle
Calling info:	None	None
Called info:	None	None
Call Timestamp:	None	
Registration server:	None	
Registration retry interval:	60sec	
Registration Timestamp:	None	None
Current Codec:	NULL	NULL
Number of calls failed:	0	0

## 7.2 SIP



The screenshot shows the AT&T Comtrend web interface. The top navigation bar includes 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. The 'SIP' tab is selected, and the 'Voice Status' page is displayed. A red arrow points to the 'SIP' tab. The 'Voice - Call Summary' table is shown below the navigation bar.

	Phone 0_0	Phone 0_1
Current Status:	Disabled	Disabled
Line Status:	Disabled	Disabled
Call State:	Idle	Idle
Calling info:	None	None
Called info:	None	None
Call Timestamp:	None	
Registration server:	None	
Registration retry interval:	60sec	
Registration Timestamp:	None	None
Current Codec:	NULL	NULL
Number of calls failed:	0	0

Click **SIP** to bring up the following window.

The settings of Global Parameters and Service Provider please contact with your ISP

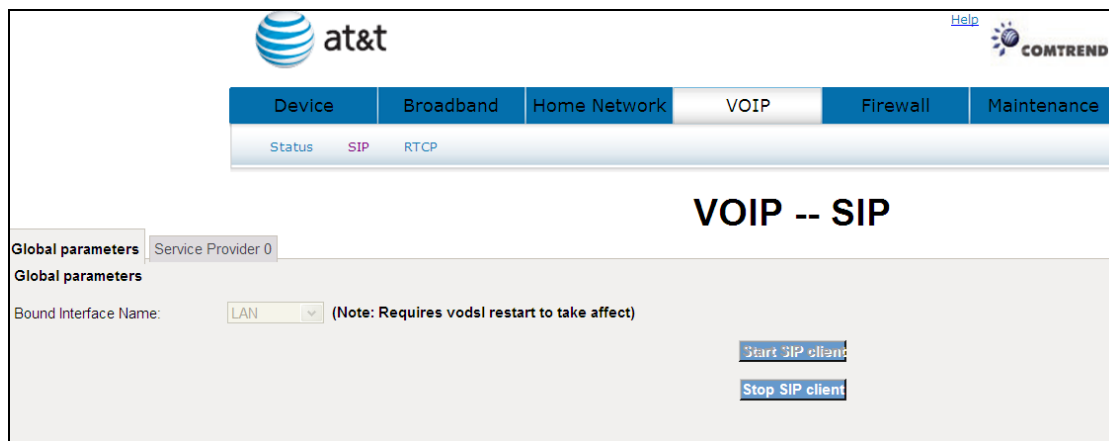
servicer.

## 7.2.1 Global Parameters

**Start SIP client:** Active SIP service (Internet telephony calls)

**Stop SIP client:** Inactive SIP service (Internet telephony calls)

About the setting of Global Parameters or want to know any detail information please contact with your ISP servicer.



A common parameter setting.

## 7.2.2 Service Provider

This screen contains basic SIP configuration settings.

**Start SIP client:** Active SIP service (Internet telephony calls)

**Stop SIP client:** Inactive SIP service (Internet telephony calls)

About the setting of Service Provider or want to know any detail information please contact with your ISP server.

VOIP -- SIP

Global parameters
Service Provider 0

Locale selection\*: USA - NORTHAMERICA (Note: Requires vodsl restart to take affect)

SIP domain name\*:

Use SIP Proxy.

SIP Proxy:

SIP Proxy port: 5060

Use SIP Outbound Proxy.

SIP Outbound Proxy:

SIP Outbound Proxy port: 5060

Use SIP Registrar.

SIP Registrar:

SIP Registrar port: 5060

SIP Account	0	1
Account Enabled	<input type="checkbox"/>	<input type="checkbox"/>
Physical Endpt Id	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="1"/>
Extension	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Display name	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Authentication name	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Preferred ptime	<span style="border: 1px solid gray; padding: 2px 5px;">20</span> ▾	<span style="border: 1px solid gray; padding: 2px 5px;">20</span> ▾
Preferred codec 1	<span style="border: 1px solid gray; padding: 2px 5px;">G.711ALaw</span> ▾	<span style="border: 1px solid gray; padding: 2px 5px;">G.711ALaw</span> ▾
Preferred codec 2	<span style="border: 1px solid gray; padding: 2px 5px;">G.729a</span> ▾	<span style="border: 1px solid gray; padding: 2px 5px;">G.729a</span> ▾
Preferred codec 3	<span style="border: 1px solid gray; padding: 2px 5px;">G.723.1</span> ▾	<span style="border: 1px solid gray; padding: 2px 5px;">G.723.1</span> ▾
Preferred codec 4	<span style="border: 1px solid gray; padding: 2px 5px;">G.726_24</span> ▾	<span style="border: 1px solid gray; padding: 2px 5px;">G.726_24</span> ▾
Preferred codec 5	<span style="border: 1px solid gray; padding: 2px 5px;">G.726_32</span> ▾	<span style="border: 1px solid gray; padding: 2px 5px;">G.726_32</span> ▾
Preferred codec 6	<span style="border: 1px solid gray; padding: 2px 5px;">GSM_AMR_12K</span> ▾	<span style="border: 1px solid gray; padding: 2px 5px;">GSM_AMR_12K</span> ▾

Start SIP client
Stop SIP client

VoIP settings are set by your service provider.



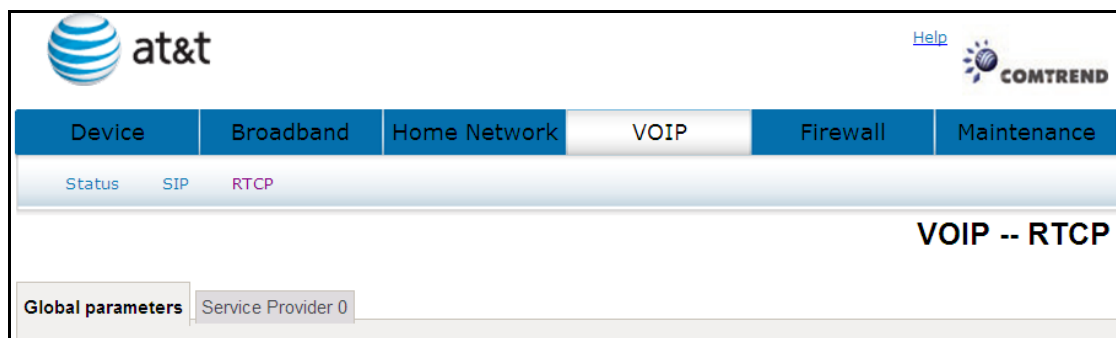
Once settings are configured, click **Start SIP client** to begin using the service.

Click **Stop SIP client** to cease using the service.

## 7.3 RTCP

For VoIP voice quality reporting, a SIP event package is specified to report RTCP and RTCP-XR summaries; SIP method options are provided to convey such events to a collector.

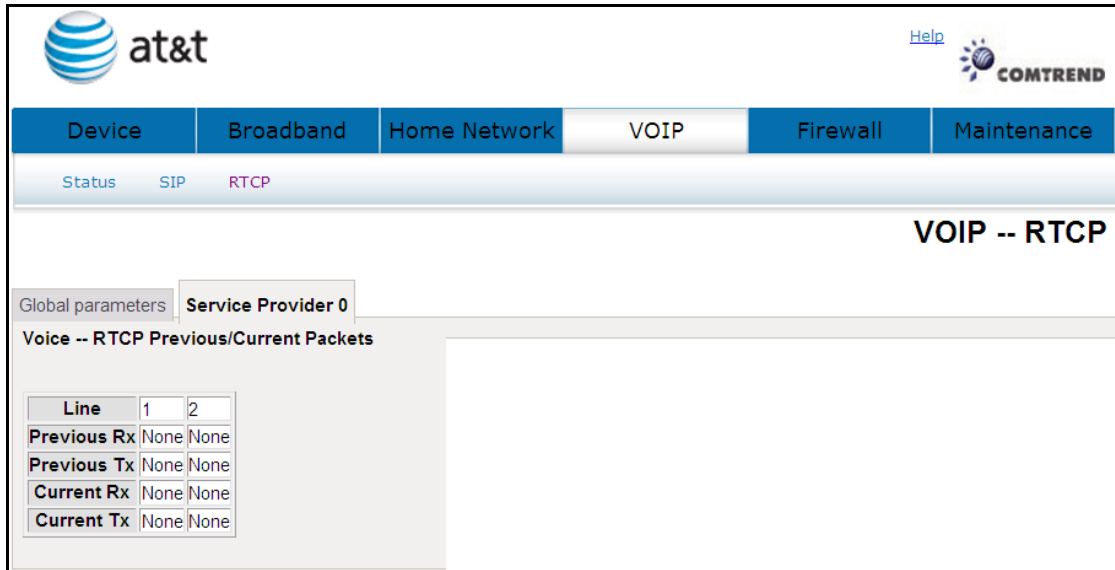
### 7.3.1 Global Parameters



A common parameter setting.

### 7.3.2 Service Provider

This screen contains basic SIP configuration settings.



NL5700 will collect and report on a set of voice quality metrics on a per-call basis to a centralized collector via SIP.

There are two primary components: First, an IETF-proposed specification is customized to define the format of a Voice Quality (VQ) report and to select metrics contained within the report. Second, two candidates SIP methods are proposed for the gateway to convey the VQ report to a third-party collector.

## 7.4 Telephone Calls

### AT&T CVoIP Star Codes

This tab is a list of star codes planned for use by AT&T CVoIP.

Code	Description
TBD	Blind Transfer - Invoke
TBD	Call Forwarding to Voice Mail - Activate
*312	Simultaneous Ringing - Activate
*313	Simultaneous Ringing - Deactivate
*370	Call Waiting - Activate (persistent)
*371	Call Waiting - Cancel (persistent)
*372	Call Forwarding Unregistered User - Activate
*373	Call Forwarding Unregistered User - Deactivate
*374	Call Forwarding Unreachable Calls to Voice Mail - Activate
*375	Call Forwarding Unreachable Calls to Voice Mail - Deactivate
*57	Customer originated Trace - Invoke
*61	Distinctive Ring Call Waiting
*63	Selective Call Forwarding - Activate
*64	Selective Call Acceptance - Activate
*66	Automatic Call Back (redial last outbound number) - Invoke
*67	Calling Line Identification - Cancel (make private)
*68	Selective Call Rejection - Activate
*69	Automatic Recall (return last incoming call) - Invoke
*70	Call Waiting - Cancel (mid call)
*70	Call Waiting - Cancel (per call)
*72	Call Forwarding (always) - Activate
*73	Call Forwarding (always) - Deactivate
*74	Speed Call Short
*75	Speed Call Long
*77	Anonymous Call Rejection - Activate
*78	Do not Disturb - Activate
*78	Call Park
*79	Do not Disturb - Deactivate
*79	Call Park Retrieve
*80	Selective Call Rejection - Deactivate

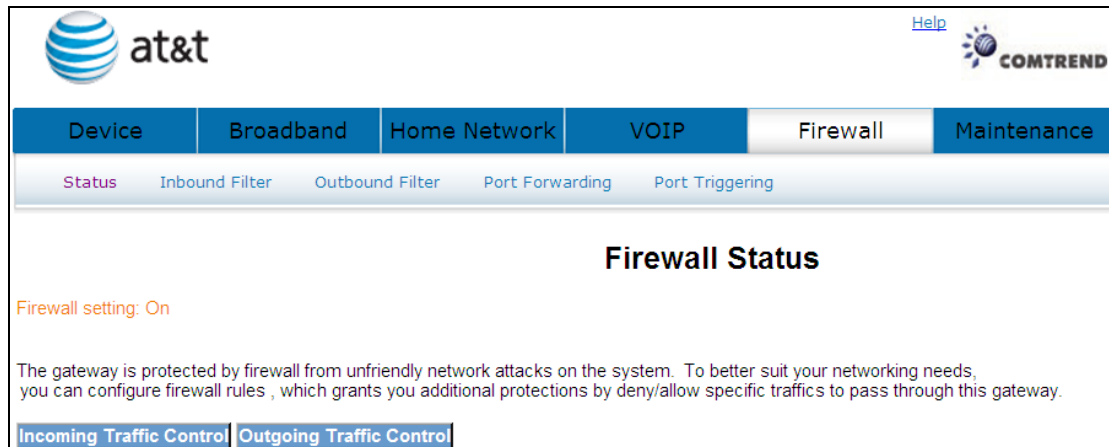
*81	Distinctive ring
*82	Calling Line Identification Restriction – Cancel (make public)
*83	Selective Call Forwarding - Deactivate
*84	Selective Call Acceptance - Deactivate
*86	Automatic Call Back Deactivate
*87	Anonymous Call Rejection - Deactivate
*89	Automatic Recall Deactivate
*90	Call Forwarding Busy - Activate
*91	Call Forwarding Busy - Deactivate
*92	Call Forwarding No Answer - Activate
*93	Call Forwarding No Answer - Deactivate
*95	Automatic Call Control VRU
*98	Voicemail
*99	Trunk Answer Any Station
N/A	Ring Back when Free (RBwF) - Cancel

## Chapter 8 Firewall

The gateway is protected by firewall from unfriendly network attacks on the system.

### 8.1 Status

Displays your firewall setting.



The screenshot shows the AT&T web interface for firewall settings. At the top left is the AT&T logo, and at the top right is the COMTREND logo with a 'Help' link. Below the logos is a navigation bar with tabs for 'Device', 'Broadband', 'Home Network', 'VOIP', 'Firewall', and 'Maintenance'. Under the 'Firewall' tab, there is a sub-menu with 'Status', 'Inbound Filter', 'Outbound Filter', 'Port Forwarding', and 'Port Triggering'. The 'Status' sub-tab is active. The main content area is titled 'Firewall Status' and displays the text: 'Firewall setting: On'. Below this, it states: 'The gateway is protected by firewall from unfriendly network attacks on the system. To better suit your networking needs, you can configure firewall rules, which grants you additional protections by deny/allow specific traffics to pass through this gateway.' At the bottom of the content area, there are two links: 'Incoming Traffic Control' and 'Outgoing Traffic Control'.

### 8.2 Inbound Filter

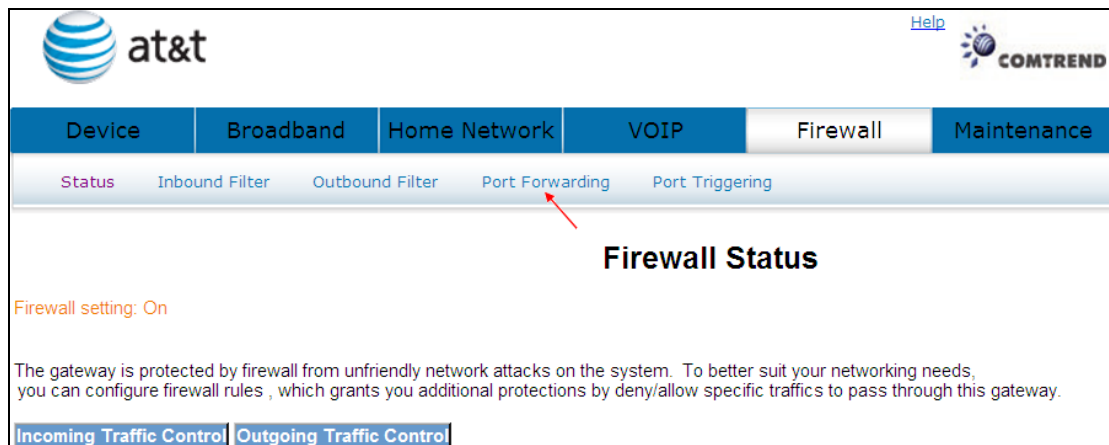
See section: [4.7.1 Incoming Traffic Control](#) for a detailed description.

### 8.3 Outbound Filter

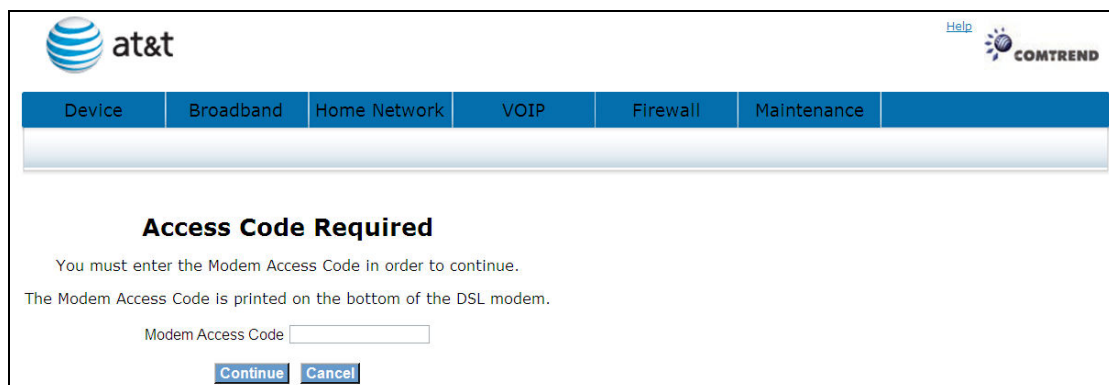
See section: [4.7.2 Outgoing Traffic Control](#) for a detailed description

## 8.4 Port Forwarding

Port forwarding allows you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the Internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.




Click **Port Forwarding** will bring up the following window.



Input the access code (which is located \_\_\_\_\_) and click the **Continue** button.

The options are shown (on the following page)

The screenshot shows the AT&T Comtrend router web interface. At the top, there are logos for AT&T and Comtrend. Below the logos is a navigation menu with tabs for Device, Broadband, Home Network, VOIP, Firewall, and Maintenance. Under the Firewall tab, there are sub-tabs for Status, Inbound Filter, Outbound Filter, Port Forwarding (which is selected), and Port Triggering. The main heading is "Port Forwarding". Below the heading is a paragraph explaining that Port Forwarding allows directing incoming traffic from the WAN side to an internal server on the LAN side. There are "Add" and "Remove" buttons. At the bottom, there is a table header with columns: Server Name, External Port Start, External Port End, Protocol, Internal Port Start, Internal Port End, Server IP Address, WAN Interface, and Remove.

Click  to display the following window.

The screenshot shows the "NAT -- Port Forwarding" configuration window. It includes a title bar, a paragraph of instructions, a note about the "Internal Port End" field, and a "Remaining number of entries that can be configured: 32" message. Below this, there are input fields for "Use Interface" (set to ipoe\_0\_1\_1.0/ptm0.0), "Service Name" (with a dropdown menu set to "Select One"), and "Server IP Address" (set to 192.168.1.). There are "Apply/Save" buttons. At the bottom, there is a table with columns: External Port Start, External Port End, Protocol, Internal Port Start, and Internal Port End. The table contains several rows, each with a dropdown menu set to "TCP".

Select a Service <b>or</b> Custom Server	User should select the service from the list. <b>or</b> User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select



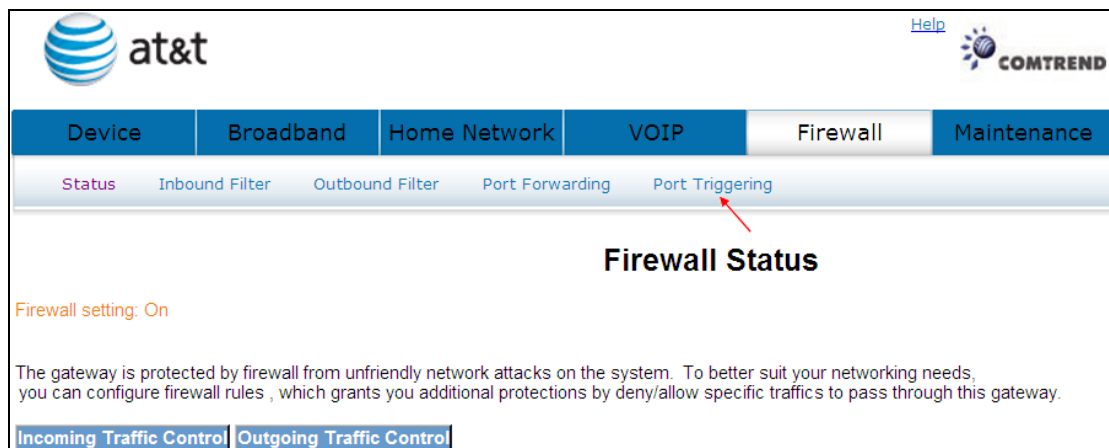
	Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

Click **Apply/Save** to forward IP packets for this service to the specified server.

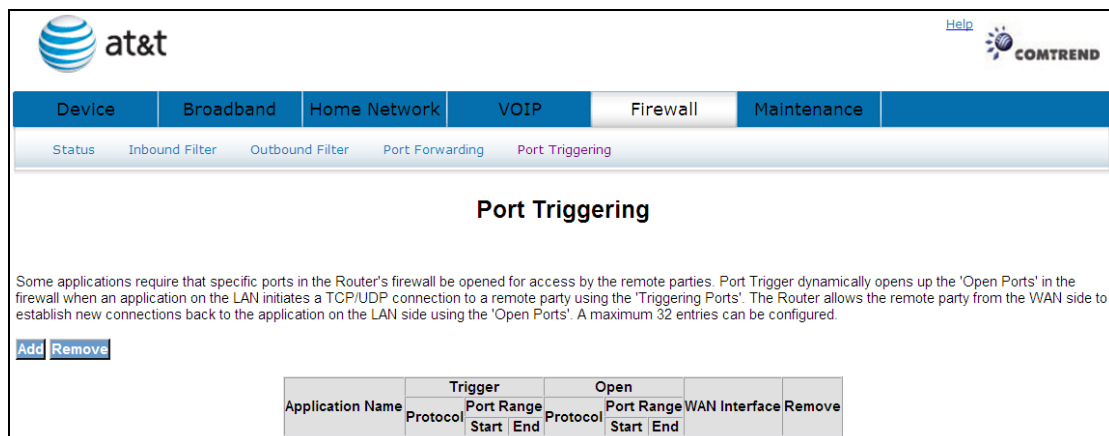
Click **Remove** to delete an entry.

## 8.5 Port Triggering

Some applications require that specific ports in the router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



Click **Port Triggering** to bring up the following window.



To add a Trigger Port, simply click **Add**. The following will be displayed.

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.  
**Remaining number of entries that can be configured: 32**

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

Select an Application <b>Or</b> Custom Application	User should select the application from the list. <b>Or</b> User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click  to add it.

Click  to delete an entry.

# Chapter 9 Maintenance

The **Diagnostics** menu provides feedback on the connection status of the device and the ADSL link. The individual tests are listed below.

## 9.1 Test

The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

at&t Help

Device Broadband Home Network VOIP Firewall Maintenance

Test DSL Ping/Traceroute/NSLookup System Log Password Upgrade Reboot Factory Reset

### Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

**Test the connection to your local network**

Test your ENET1 Connection:	FAIL	<a href="#">Help</a>
Test your ENET2 Connection:	FAIL	<a href="#">Help</a>
Test your ENET3 Connection:	FAIL	<a href="#">Help</a>
Test your ENET4 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>

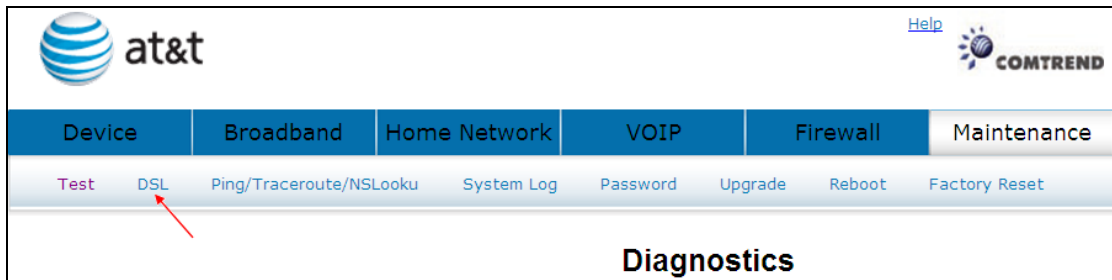
**Test the connection to your DSL service provider**

Test xDSL Synchronization:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	DISABLED	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	DISABLED	<a href="#">Help</a>

[Rerun Diagnostic Tests](#) [Test With OAM F4](#)

If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures. To test the connection with your DSL service provider, click **Test With OAM F4**

## 9.2 DSL



Click **DSL** to display the xDSL Diagnostics window.

### Diagnostics -- xDSL Statistics

Bonding Line Selection  ▼

Mode:		
Traffic Type:		
Status:		Disabled
Link Power State:		
	<b>Downstream</b>	<b>Upstream</b>
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

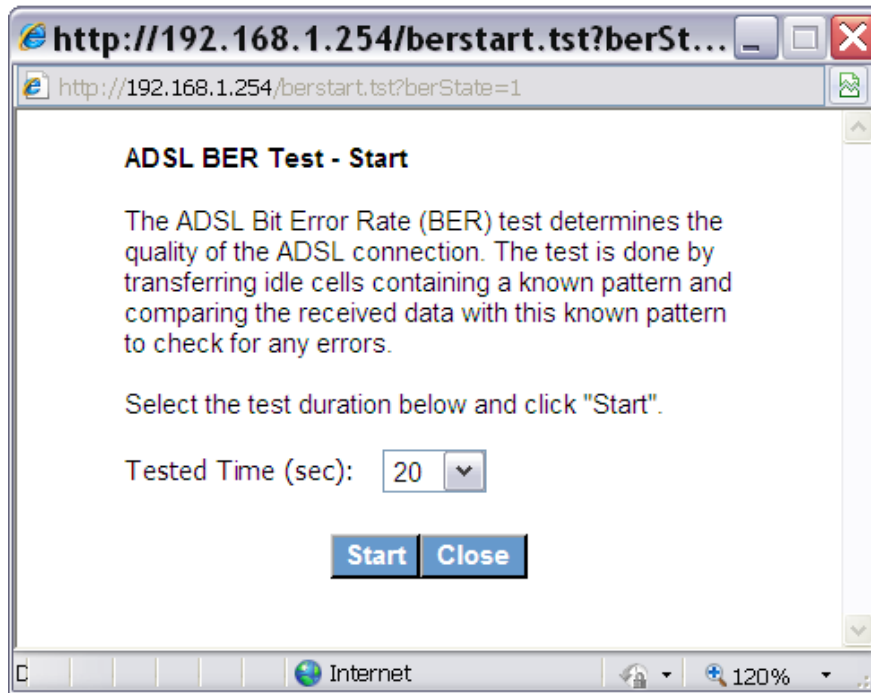
Consult the table below for descriptions of each field.

<b>Field</b>	<b>Description</b>
Mode	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2
Traffic Type	Channel type Interleave or Fast
Status	Lists the status of the DSL link
Link Power State	Link output power state.
Line Coding	Trellis On/Off
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

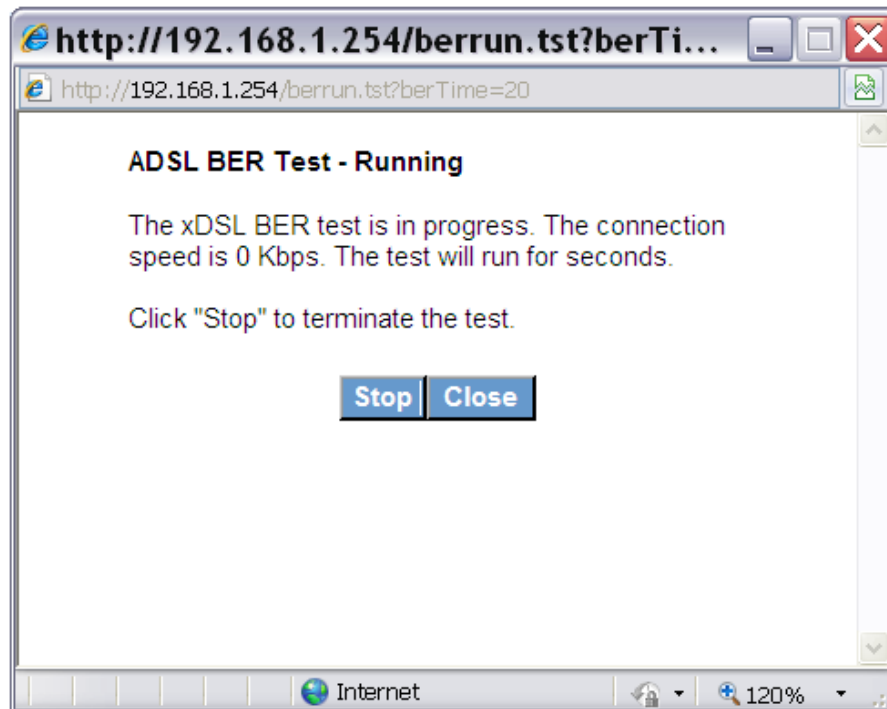
### 9.2.1 xDSL BER Test

Click [xDSL BER Test](#) on the xDSL Statistics screen to test the Bit Error Rate

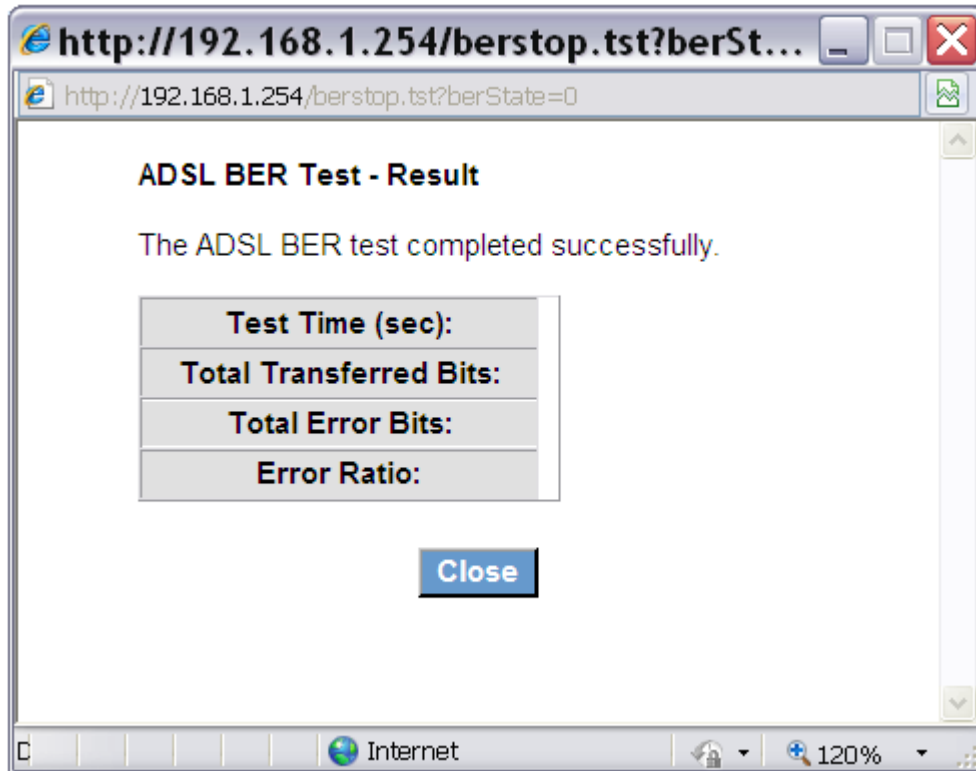
(BER). A small pop-up window will open after the button is pressed, as shown below.



Click **Start** to start the test or click **Close** to cancel the test.



After the BER testing is complete, the pop-up window will display as follows.



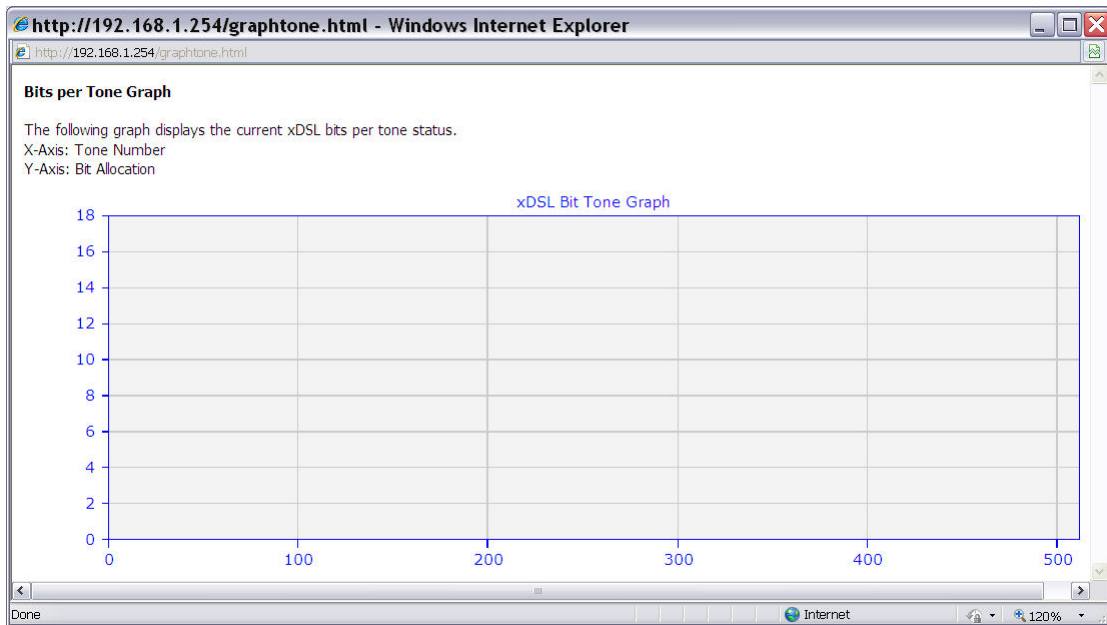
### 9.2.2 Reset Statistics

Click [Reset Statistics](#) to refresh the screen.

### 9.2.3 Draw Graph Tone

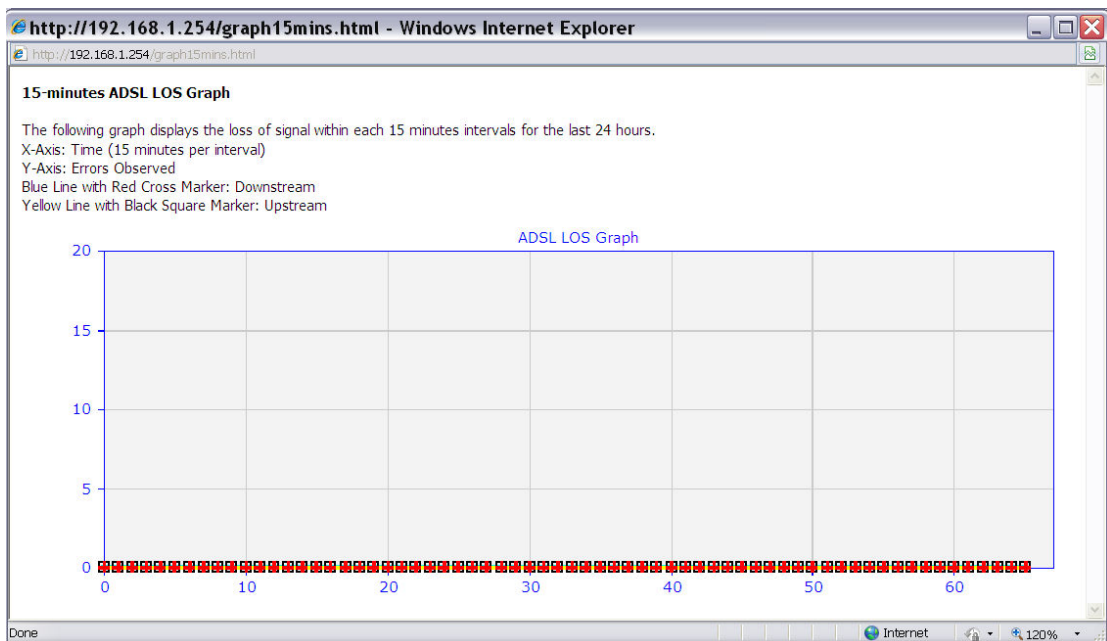
Click [Draw Tone Graph](#) to display the current xDSL bits per tone status. The X axis represents Tone Number and the Y axis represents Bit Allocation.





### 9.2.4 Draw Loss of Signal Graph

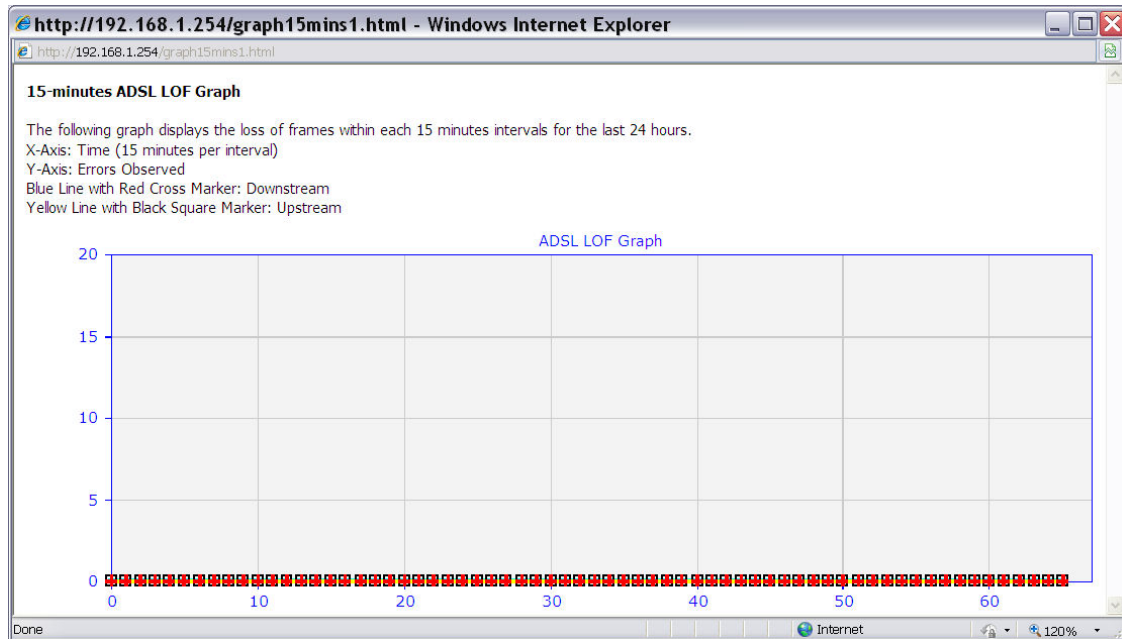
Click **Draw LOS Graph** to display the loss of signal within each 15 minute intervals for the last 24 hours. The X axis represents Time and the Y axis represents Errors Observed.



### 9.2.5 Draw Loss of Frames Graph

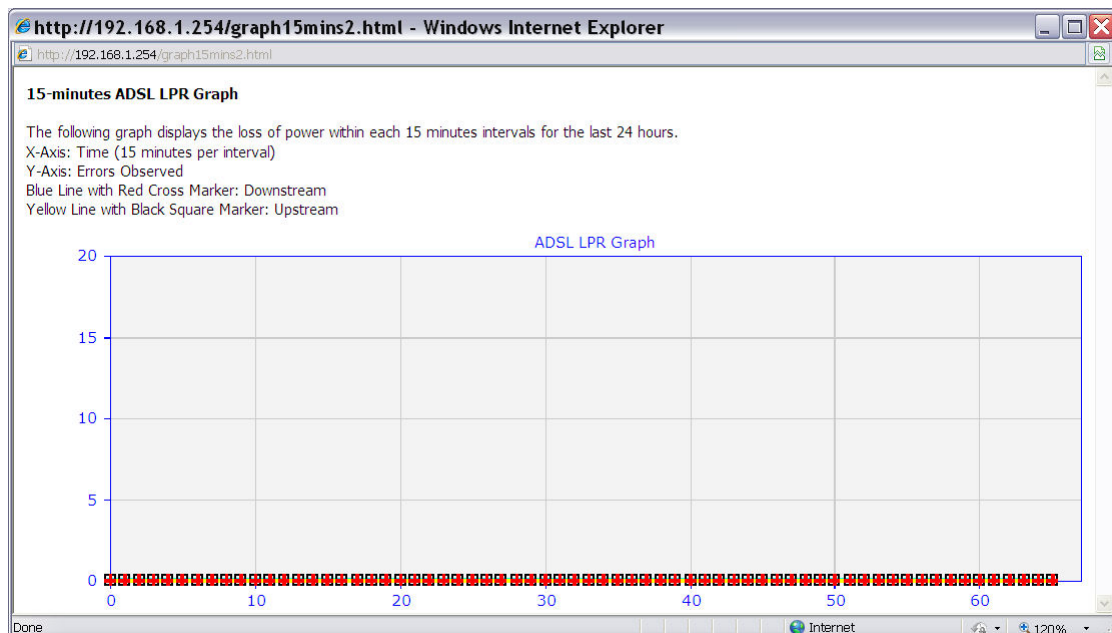
Click **Draw LOF Graph** to display the loss of frames within each 15 minute

intervals for the last 24 hours. The X axis represents Time and the Y axis represents Errors Observed.

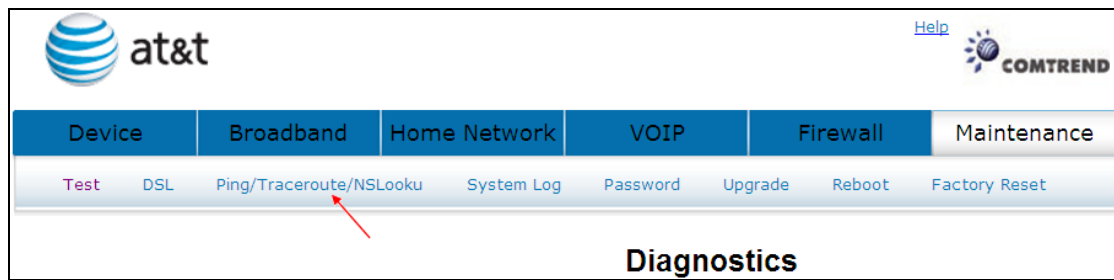


## 9.2.6 Loss of Power

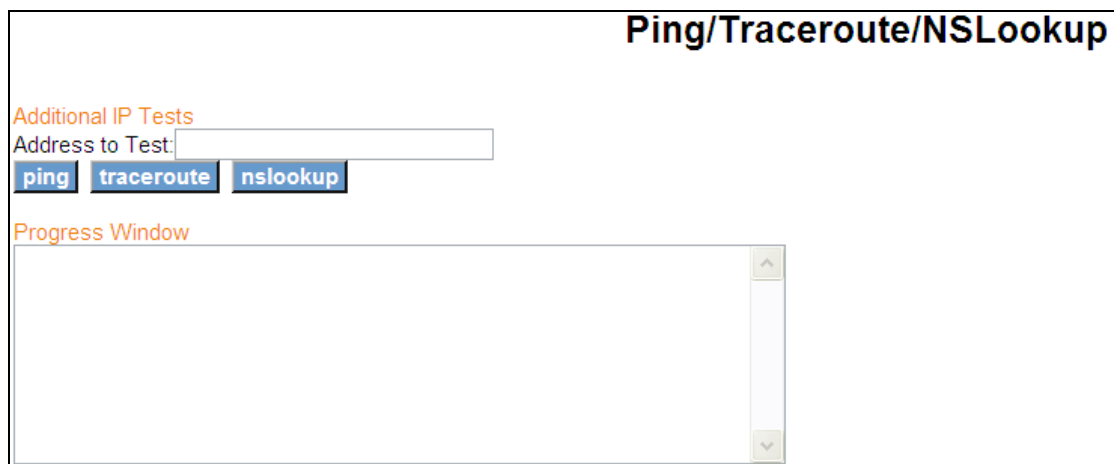
Click **Draw LPR Graph** to display the loss of power within each 15 minute intervals for the last 24 hours. The X axis represents Time and the Y axis represents Errors Observed.



## 9.3 Ping/Traceroute/NSLookup

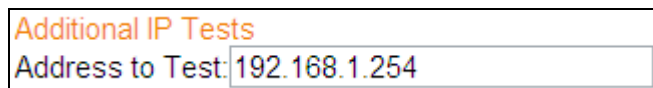


Click **Ping/Traceroute/NSLookup** to bring up the following window.



### 9.3.1 Ping

Ping: Used to test the reach ability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer



Click **ping** to seek a reply from an IP address.

### Progress Window

```
PING 192.168.1.254 (192.168.1.254): 56 data bytes
56 bytes from 192.168.1.254: icmp_seq=0 ttl=64 time=0.3 ms
56 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.2 ms
56 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.2 ms
```

## 9.3.2 TraceRoute

TraceRoute: Used to show the route taken by packets across an IP network. Traceroute is often used for network troubleshooting. By showing a list of routers traversed, it allows the user to identify the path taken to reach a particular destination on the network.

### Additional IP Tests

Address to Test:

Click **traceroute** to trace the route of an IP address.

### Progress Window

```
1 192.168.1.254 (192.168.1.254) 0.245 ms 0.169 ms 0.153 ms
traceroute: 192.168.1.254
: Unknown host
```

## 9.3.3 NSLookup

Nslookup: Used to query Domain Name System (DNS) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain.

**Additional IP Tests**  
Address to Test:

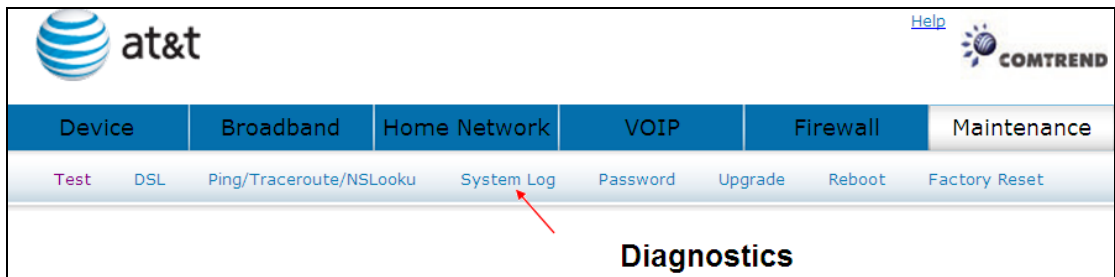
Click **nslookup** to lookup the name server of an IP address.

**Progress Window**

```
set timeout = 1 (sec)
set repetitions = 1
*** Unknown host
```

## 9.4 System Log

The System Log option allows you to view the system events log.



Click **System Log** to bring up the following window.

<b>System Log</b>			
		<a href="#">Refresh</a>	<a href="#">Export Syslog</a>
Date/Time	Facility	Severity	Message
P0000-00-00T06:06:49	user	warn	kernel: PLL init completed. PLL registers set to:
P0000-00-00T06:06:49	user	warn	kernel: PCM->pcm_pl_ctrl1 = 0x0080147D
P0000-00-00T06:06:49	user	warn	kernel: PCM->pcm_pl_ctrl2 = 0x10000000
P0000-00-00T21:00:12	syslog	info	-- MARK --
P0000-00-00T22:00:12	syslog	info	-- MARK --
P0000-00-00T23:00:12	syslog	info	-- MARK --
P0000-00-01T00:00:12	syslog	info	-- MARK --
P0000-00-01T00:34:25	user	crit	kernel: eth3 Link UP 100 mbps full duplex
P0000-00-01T00:34:25	user	info	kernel: br0: port 4(eth3) entering learning state
P0000-00-01T00:34:25	user	info	kernel: br0: topology change detected, propagating
P0000-00-01T00:34:25	user	info	kernel: br0: port 4(eth3) entering forwarding state
P0000-00-01T01:00:12	syslog	info	-- MARK --
P0000-00-01T01:38:24	user	crit	kernel: eth3 Link DOWN.
P0000-00-01T01:38:24	user	info	kernel: br0: port 4(eth3) entering disabled state
P0000-00-01T02:00:12	syslog	info	-- MARK --
P0000-00-01T03:00:12	syslog	info	-- MARK --
P0000-00-01T04:00:12	syslog	info	-- MARK --
P0000-00-01T04:12:56	user	crit	kernel: eth3 Link UP 100 mbps full duplex
P0000-00-01T04:12:56	user	info	kernel: br0: port 4(eth3) entering learning state
P0000-00-01T04:12:56	user	info	kernel: br0: topology change detected, propagating
P0000-00-01T04:12:56	user	info	kernel: br0: port 4(eth3) entering forwarding state

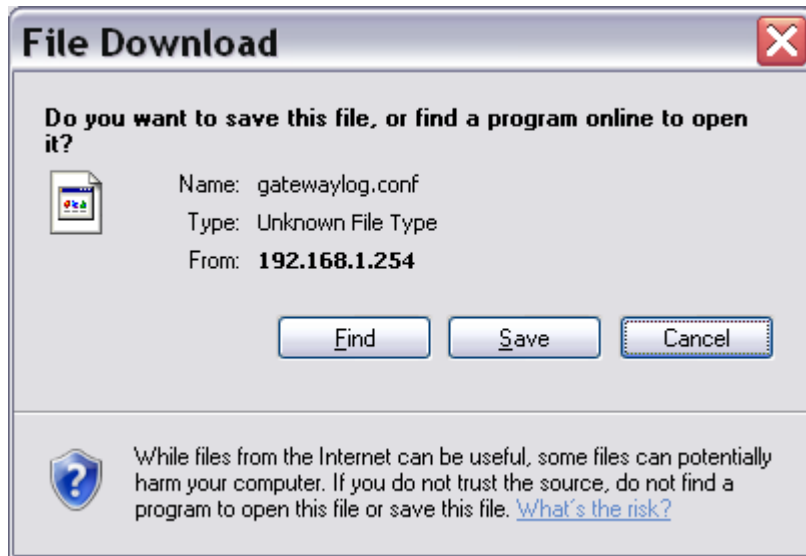
[Refresh](#)   [Export Syslog](#)


### 9.4.1 Refresh

Click [Refresh](#) to update the System Log.

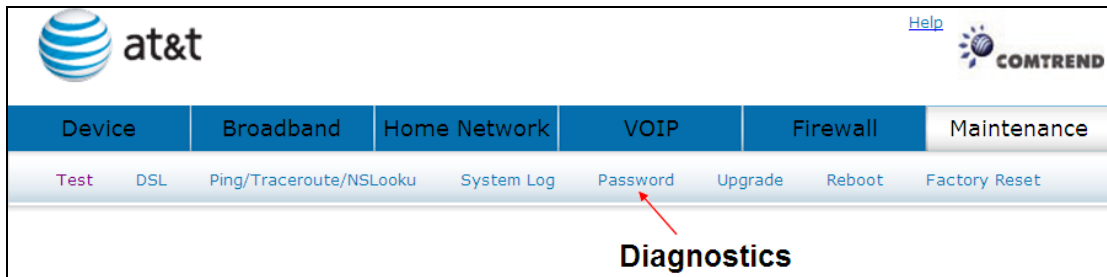
### 9.4.2 Export Syslog

Click [Export Syslog](#) to bring up the following window.

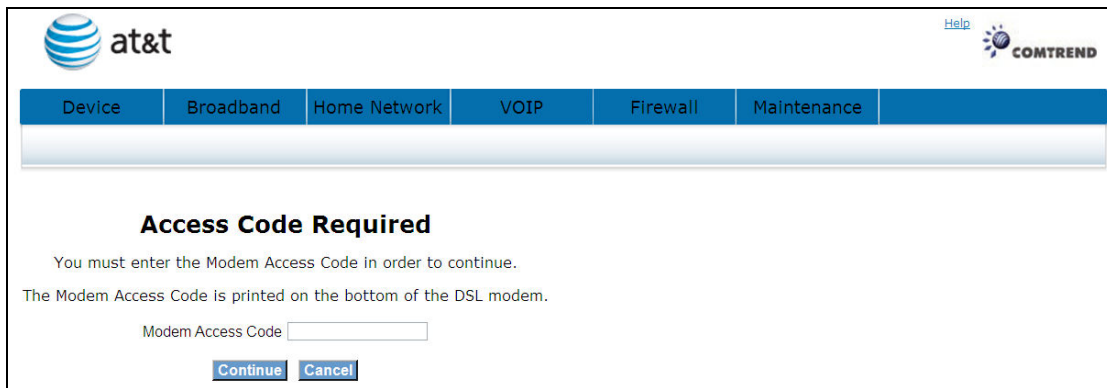


Click  to save the system log file.

## 9.5 Password

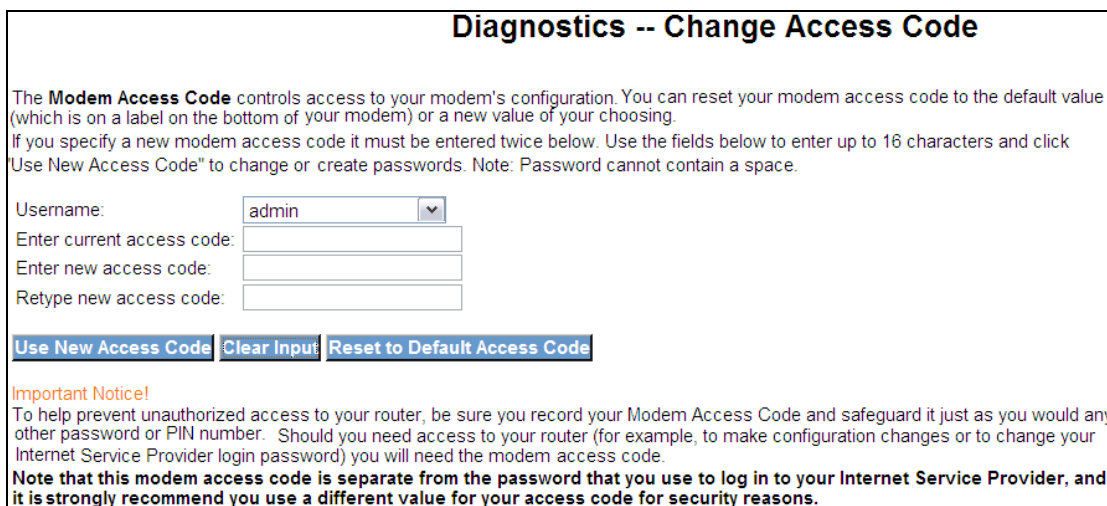


Click **Password** to bring up the following window.



Input the access code (which is located \_\_\_\_\_) and click **Continue**

The options are shown (on the following page)





### **9.5.1 Use New Access Code**

Select User, enter the current access code and the new access code. Then retype the new access code.

Click [Use New Access Code](#)

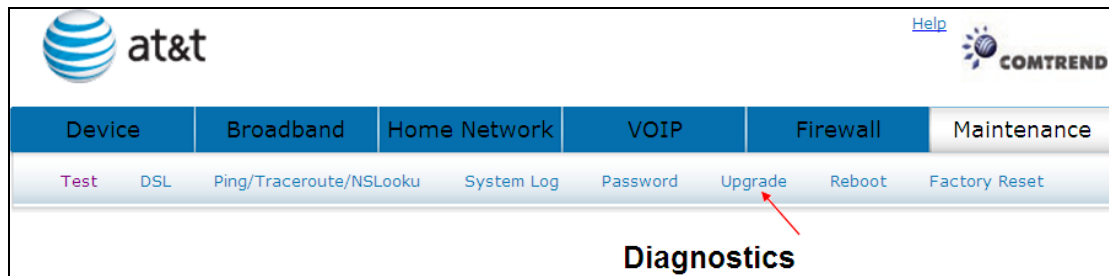
### **9.5.2 Clear Input**

Click [Clear Input](#) to delete what you have entered.

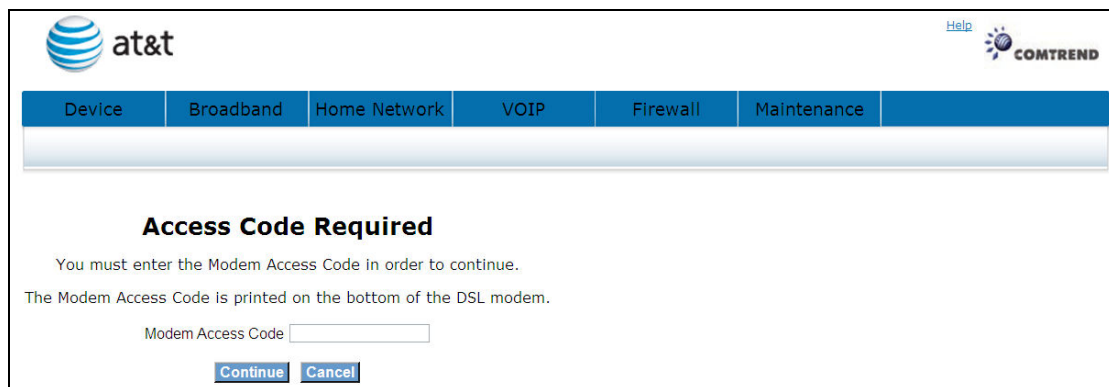
### **9.5.3 Reset to Default Access Code**

Click [Reset to Default Access Code](#) to reset to default.

## 9.6 Upgrade

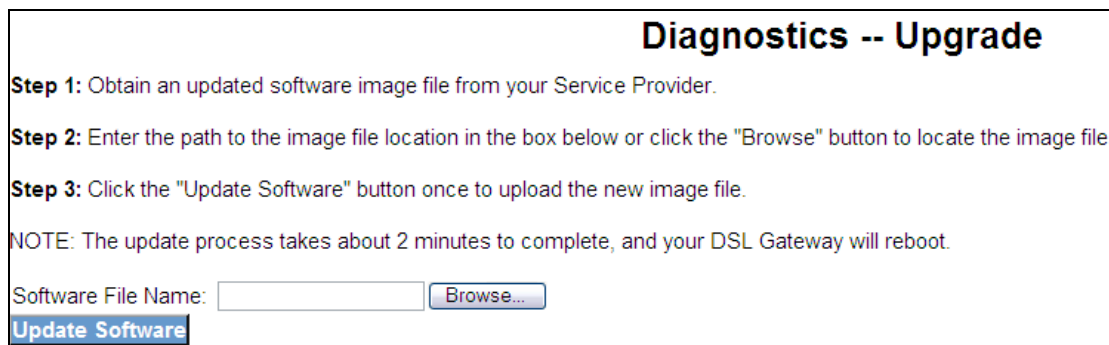


Click **Upgrade** to bring up the following window.



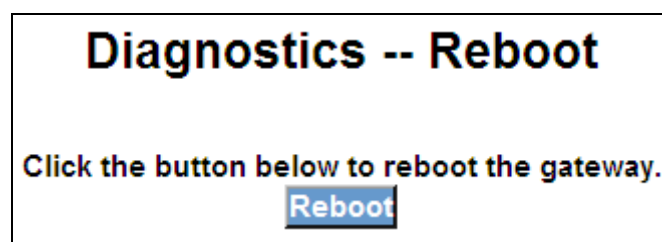
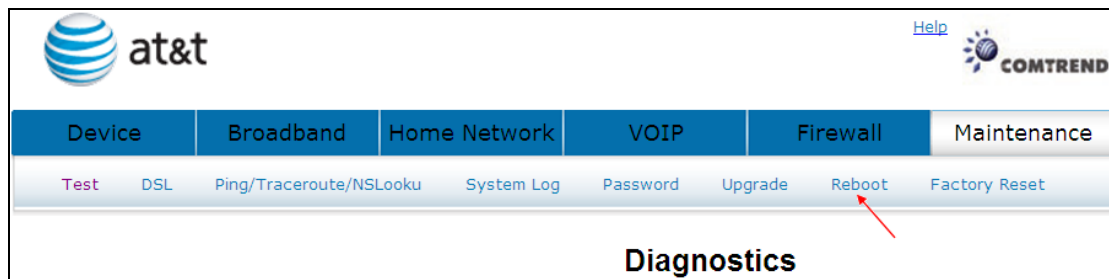
Input the access code (which is located \_\_\_\_\_) and click **Continue**

The options are shown (on the following page)



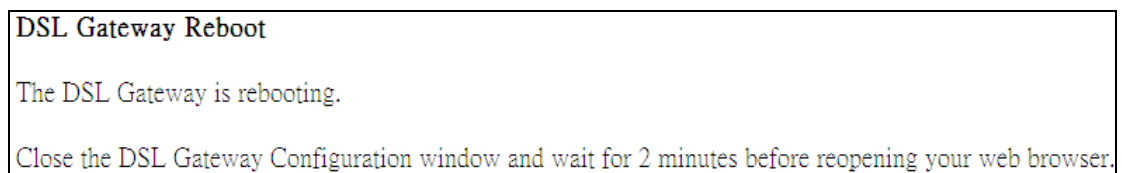
Click **Update Software** to start the upgrade process.

## 9.7 Reboot

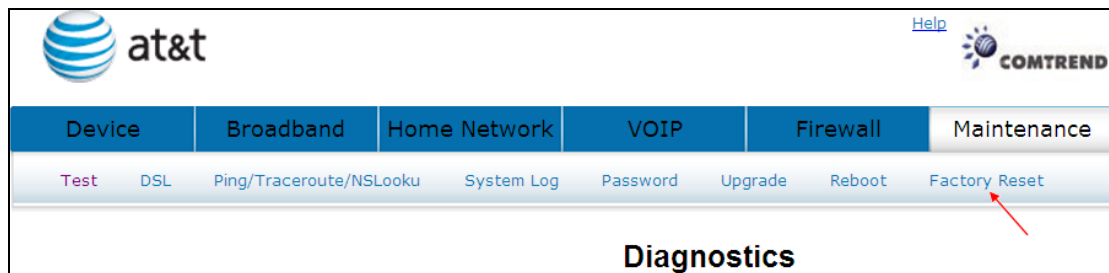


Click **Reboot** to reboot the gateway.

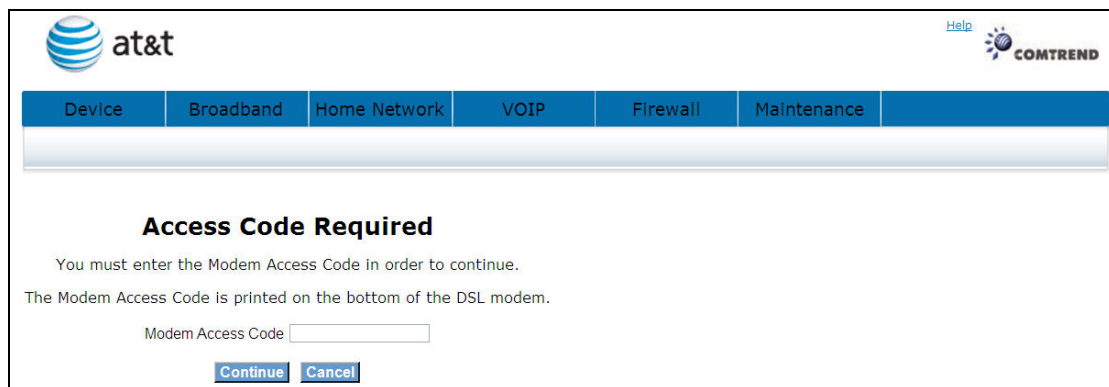
The following window will be displayed.



## 9.8 Factory Reset



Click **Factory Reset** to bring up the following window.

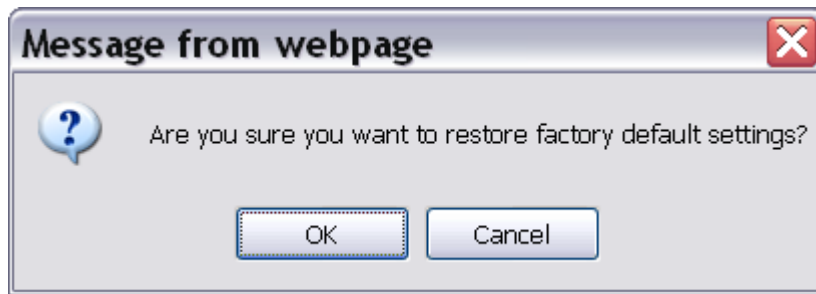


Input the access code (which is located \_\_\_\_\_) and click **Continue**

The options are shown (on the following page)



Click **Restore Default Settings** to restore the DSL gateway to the factory defaults.



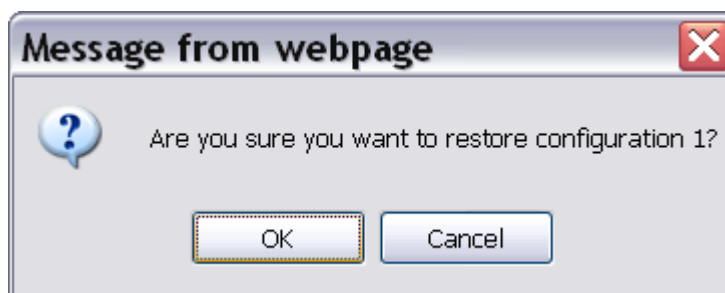
Click **OK** to confirm.

**DSL Gateway Restore**

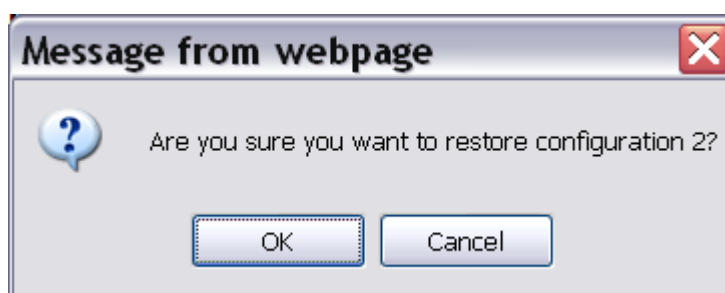
The DSL Gateway configuration has been restored to default settings and the router is rebooting.

Close the DSL Gateway Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

#### Restore configuration 1



#### Restore configuration 2



Click **OK** to confirm.

# Appendix A: Firewall

## Stateful Packet Inspection

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

## Denial of Service attack

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

## TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3. When a Routing interface is created "Enable Firewall" must be checked. Navigate to Advanced Setup -> Security -> IP Filtering, web page.

Outbound Filter: Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

**Filter Name:** User defined Filter Name.

**Protocol:** Can take on any values from: TCP/UDP, TCP, UDP or ICMP

**Source IP Address/Source Subnet Mask:** Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

**Source Port:** This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

**Destination IP Address/Destination Subnet Mask:** Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.

**Destination Port:** This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

**Examples:**

1. Filter Name : Out\_Filter1  
Protocol : TCP  
Source Address : 192.168.1.45  
Source Subnet Mask : 255.255.255.0  
Source Port : 80  
Dest. Address : NA  
Dest. Sub. Mask : NA  
Dest. Port : NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2. Filter Name : Out\_Filter2  
Protocol : UDP  
Source Address : 192.168.1.45  
Source Subnet Mask : 255.255.255.0  
Source Port : 5060:6060  
Dest. Address : 172.16.13.4  
Dest. Sub. Mask : 255.255.255.0  
Dest. Port : 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070

**Inbound Filter:**Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IP traffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

**Filter Name:** User defined Filter Name.

**Protocol:** Can take on any values from: TCP/UDP, TCP, UDP or ICMP

**Source IP Address/Source Subnet Mask:** Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

**Source Port:** This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

**Destination IP Address/Destination Subnet Mask:** Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

**Destination Port:** This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

**Examples:**

1. Filter Name : In\_Filter1  
Protocol : TCP  
Source Address : 210.168.219.45  
Source Subnet Mask : 255.255.0.0  
Source Port : 80  
Dest. Address : NA  
Dest. Sub. Mask : NA  
Dest. Port : NA

Selected WAN interface: mer\_0\_35/nas\_0\_35

This filter will ACCEPT all TCP packets coming from WAN interface mer\_0\_35/nas\_0\_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.



2. Filter Name : In\_Filter2  
Protocol : UDP  
Source Address : 210.168.219.45  
Source Subnet Mask : 255.255.0.0  
Source Port : 5060:6060  
Dest. Address :192.168.1.45  
Dest. Sub. Mask : 255.255.255.0  
Dest. Port : 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer\_0\_35/nas\_0\_35 with IP Address/Sub. Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

## Appendix B: Pin Assignments

### Line port (RJ14)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP1
2	ADSL_TIP2	5	ADSL_RING2
3	ADSL_RING1	6	-

### LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

## Appendix C: Specifications

### Rear Panel

RJ-14 X1 for ADSL2+ bonded, RJ-45 X 4 for LAN, Reset Button X 1,  
WPS button x1, WIFI button x1 Wi-Fi Antenna x 1

### ADSL

ADSL standard	ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2AnnexM
ADSL2 Bonded	Downstream : 48 Mbps Upstream : 2.6 Mbps
ADSL2+ Bonded	Downstream : 48 Mbps Upstream : 2.6 Mbps
ADSL2+ non-Bonded	Downstream : 24 Mbps Upstream : 1.3 Mbps
ADSL2 non-Bonded	Downstream : 12 Mbps Upstream : 1.3 Mbps
G.DMT	Downstream : 8Mbps Upstream : 832kbps

### LAN

Standard	IEEE 802.3, IEEE 802.3u
10/100 BaseT	Auto-sense
MDI/MDX support	Yes

### Wireless

Standard	IEEE802.11b/g/n, backward compatible with 802.11b
Encryption	64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
Channels	11 Channels (US, Canada)

Data Rate Up to 300Mbps

BSSID Multiple

WPA Yes

WPA2 Yes

WEP Yes

WDS Yes

IEEE 802.1x Yes

10,25,50,100mW@22MHz channel bandwidth output power level can be

selected according to the environment

### **ATM Attributes**

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);  
RFC 1577 (IPoA)  
Support PVCs 16  
AAL type AAL5  
ATM service class UBR/CBR/VBR-rt/VBR-nrt  
ATM UNI support UNI3.1/4.0  
OAM F4/F5 Yes

### **Management**

SNMP, Telnet, Web-based management, Configuration backup and restoration  
Software upgrade via HTTP, TFTP server, or FTP server  
Supports TR-069/TR-098/TR-111 for Remote Management

### **Bridge Functions**

Transparent bridging and learning	IEEE 802.1d
VLAN support	Yes
Spanning Tree Algorithm	Yes
IGMP Proxy	Yes
IGMP Snooping	Yes

### **Voice**

SIP: RFC 3261  
Codec: G.711, G.723.1, G.726, G.729ab  
RTP: RFC 1889  
SDP: RFC 2327  
Caller ID: ETSI based

### **Routing Functions**

Static route, RIP, and RIPv2, NAT/PAT, DHCP Server/DHCP Relay, DNS Relay, ARP

### **Security Functions**

Authentication protocols PAP, CHAP,  
TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet and MAC address  
filtering, SSH

**Application Passthrough**

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc

**OS Supported for USB driver**

Windows 2000/XP/ME/98SE

**Power Supply**

External power adapter 100-240Vac

**Environment Condition**

Operating temperature 0 ~ 40 degrees Celsius

Relative humidity 5 ~ 95% (non-condensing)

**Dimensions**

205 mm (W) x 48 mm (H) x 145 mm (D)

**Certifications**

FCC Part 15 class B, FCC Part 68, CE

**Kit Weight**

0.98 KG

**NOTE:** Specifications are subject to change without notice

## Appendix D: SSH Client

Linux OS comes with ssh client. Microsoft Windows does not have ssh client but there is a public domain one "putty" that you can download.

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

### **To access the router using Linux ssh client:**

From LAN: Use the router WEB UI to enable SSH access from LAN.

(default is enabled)

type: `ssh -l admin 192.168.1.1`

From WAN: In the router, use WEB UI to enable SSH access from WAN.

type: `ssh -l support router-WAN-ip-address`

### **To access the router using Windows putty ssh client:**

From LAN: Use the router WEB UI to enable SSH access from LAN

(default is enabled)

type: `putty -ssh -l admin 192.168.1.1`

From WAN: In the router, use WEB UI to enable SSH access from WAN.

type: `putty -ssh -l support router-WAN-ip-address`