

MAX-207HW2R

WiMAX MIMO Indoor Simple CPE (2.5 GHz)

User's Guide



Default Login Details

IP Address	http://192.168.1.1
Admin Name and Password	admin 1234
User Name and Password	User user

Firmware Version 1.0
Edition 1, 02/2010

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL MAX-207HW2R using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

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

- Web Configurator Online Help

Embedded web help for descriptions of individual screens and supplementary information.

- Command Reference Guide

The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the MAX-207HW2R.

Note: It is recommended you use the web configurator to configure the MAX-207HW2R.

- Support Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

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

Documentation Feedback

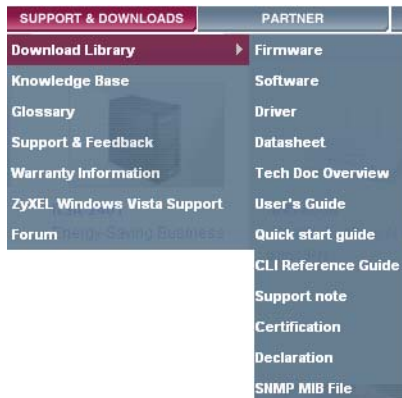
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- **Download Library**

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- **Knowledge Base**

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- **Forum**

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

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

Warnings tell you about things that could harm you or your MAX-207HW2R.

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





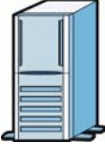







Syntax Conventions

- The MAX-207HW2R may be referred to as the "MAX-207HW2R", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **TOOLS > Logs > Log Settings** means you first click **Tools** in the navigation panel, then the **Logs** sub menu and finally the **Log Settings** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The MAX-207HW2R icon is not an exact representation of your MAX-207HW2R.\

Table 1 Common Icons

<p>WiMAX Device</p> 	<p>WiMAX Access Point</p> 	<p>Computer</p> 
<p>Notebook</p> 	<p>Server</p> 	<p>WiMAX Base Station</p> 
<p>Telephone</p> 	<p>Switch</p> 	<p>Router</p> 
<p>Internet Cloud</p> 	<p>Internet/WiMAX Cloud</p> 	<p>Wireless Signal</p> 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one. Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device. Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- Make sure that the cable system is grounded so as to provide some protection against voltage surges.

Your product is marked with this symbol, which is known as the WEEE mark.

WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

User's Guide	17
Getting Started	19
Introducing the Web Configurator	23
Technical Reference	29
The Setup Screens	31
The Status Screen	39
The LAN Configuration Screens	43
The WIFI Configuration Screen	55
The WAN Configuration Screens	71
The Port Configuration Screens	83
The System Configuration Screens	89
The Service Configuration Screens	97
The Phone Screens	111
The Phone Book Screens	121
The Certificates Screens	127
The Remote Management Screens	135
The Firewall Screens	145
Content Filter	155
The Password Setup Screen	159
The Status Screen	161
Troubleshooting	165
Product Specifications	173

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
Contents Overview	9
Table of Contents.....	11
Part I: User's Guide.....	17
Chapter 1	
Getting Started	19
1.1 About Your MAX-207HW2R	19
1.1.1 WiMAX Internet Access	19
1.1.2 Make Calls via Internet Telephony Service Provider	20
1.2 MAX-207HW2R Hardware	21
1.2.1 LEDs	21
1.3 Good Habits for Managing the MAX-207HW2R	22
Chapter 2	
Introducing the Web Configurator	23
2.1 Overview	23
2.1.1 Accessing the Web Configurator	23
2.1.2 The Reset Button	24
2.2 The Main Screen	25
Part II: Technical Reference	29
Chapter 3	
The Setup Screens.....	31
3.1 Overview	31
3.1.1 What You Can Do in This Chapter	31
3.1.2 What You Need to Know	31
3.1.3 Before You Begin	32
3.2 LAN Configuration	32

3.3 DHCP Client	33
3.4 Time Setting	35
3.4.1 Pre-Defined NTP Time Servers List	36
3.4.2 Resetting the Time	37
Chapter 4	
The Status Screen.....	39
4.1 Overview	39
4.2 Status Screen	39
Chapter 5	
The LAN Configuration Screens.....	43
5.1 Overview	43
5.1.1 What You Can Do in This Chapter	43
5.1.2 What You Need to Know	43
5.2 DHCP Setup	44
5.3 Static DHCP	45
5.4 IP Alias	47
5.5 Advanced	49
5.6 Technical Reference	50
5.6.1 IP Address and Subnet Mask	50
5.6.2 DHCP Setup	51
5.6.3 LAN TCP/IP	51
5.6.4 DNS Server Address	51
5.6.5 RIP Setup	52
5.6.6 Multicast	53
Chapter 6	
The WIFI Configuration Screen	55
6.1 Overview	55
6.1.1 What You Can Do in the WIFI Screens	55
6.1.2 What You Need to Know About WIFI	56
6.1.3 Before You Start	59
6.2 General Screen	59
6.2.1 No Security	60
6.2.2 WEP Encryption	61
6.2.3 WPA(2)-PSK	62
6.2.4 Wireless LAN Advanced Setup	63
6.3 MAC Filter	64
6.4 WPS	65
6.5 Wireless LAN Technical Reference	66
6.5.1 Additional Wireless Terms	66
6.5.2 Wireless Security Overview	66

6.5.3 WiFi Protected Setup	68
Chapter 7	
The WAN Configuration Screens.....	71
7.1 Overview	71
7.1.1 What You Can Do in This Chapter	71
7.1.2 What You Need to Know	71
7.2 Internet Connection	73
7.3 WiMAX Configuration	75
7.3.1 Frequency Ranges	78
7.3.2 Configuring Frequency Settings	78
7.4 WiMAX FC Table	80
Chapter 8	
The Port Configuration Screens.....	83
8.1 Overview	83
8.1.1 What You Can Do in This Chapter	83
8.2 General	84
8.3 Port Forwarding	85
8.3.1 Port Forwarding Options	85
8.3.2 Port Forwarding Rule Setup	87
Chapter 9	
The System Configuration Screens	89
9.1 Overview	89
9.1.1 What You Can Do in This Chapter	89
9.1.2 What You Need to Know	89
9.2 Dynamic DNS	90
9.3 Firmware	92
9.3.1 The Firmware Upload Process	93
9.4 Configuration	93
9.4.1 The Restore Configuration Process	94
9.5 Restart	95
9.5.1 The Restart Process	95
Chapter 10	
The Service Configuration Screens	97
10.1 Overview	97
10.1.1 What You Can Do in This Chapter	97
10.1.2 What You Need to Know	97
10.1.3 Before you Begin	99
10.2 SIP Settings	99
10.2.1 Advanced SIP Settings	100

10.3 Technical Reference	106
10.3.1 SIP Call Progression	106
10.3.2 SIP Client Server	107
10.3.3 SIP User Agent	107
10.3.4 SIP Proxy Server	107
10.3.5 SIP Redirect Server	108
10.3.6 NAT and SIP	109
10.3.7 DiffServ	109
10.3.8 DSCP and Per-Hop Behavior	110
Chapter 11	
The Phone Screens.....	111
11.1 Overview	111
11.1.1 What You Can Do in This Chapter	111
11.1.2 What You Need to Know	111
11.2 Analog Phone	112
11.2.1 Advanced Analog Phone Setup	113
11.3 Common	115
11.4 Region	116
11.5 Technical Reference	116
11.5.1 The Flash Key	117
11.5.2 Europe Type Supplementary Phone Services	117
11.5.3 USA Type Supplementary Services	119
Chapter 12	
The Phone Book Screens.....	121
12.1 Overview	121
12.1.1 What You Can Do in This Chapter	121
12.1.2 What You Need to Know	121
12.2 Call Forward Policy	122
12.3 Speed Dial	124
12.3.1 Speed Dial Setup	125
Chapter 13	
The Certificates Screens	127
13.1 Overview	127
13.1.1 What You Can Do in This Chapter	127
13.1.2 What You Need to Know	127
13.2 My Certificates	128
13.3 Trusted CAs	129
13.4 Technical Reference	129
13.4.1 Certificate Authorities	130
13.4.2 Verifying a Certificate	132

Chapter 14	
The Remote Management Screens	135
14.1 Overview	135
14.1.1 What You Can Do in This Chapter	135
14.1.2 What You Need to Know	136
14.2 WWW	137
14.3 Telnet	138
14.4 FTP	139
14.5 SNMP	140
14.5.1 SNMP Traps	141
14.5.2 SNMP Options	142
14.6 DNS	143
14.7 Ping	144
Chapter 15	
The Firewall Screens	145
15.1 Overview	145
15.1.1 What You Can Do in This Chapter	145
15.1.2 What You Need to Know	145
15.2 Firewall Setting	146
15.2.1 Firewall Rule Directions	146
15.2.2 Triangle Route	147
15.2.3 Firewall Setting Options	148
15.3 Services	149
15.4 Technical Reference	151
15.4.1 Stateful Inspection Firewall.	151
15.4.2 Guidelines For Enhancing Security With Your Firewall	151
15.4.3 The “Triangle Route” Problem	151
Chapter 16	
Content Filter.....	155
16.1 Overview	155
16.1.1 What You Can Do in This Chapter	155
16.2 Filter	156
16.3 Schedule	158
Chapter 17	
The Password Setup Screen.....	159
17.1 Overview	159
17.2 Password Setup	159
Chapter 18	
The Status Screen.....	161

18.1 Overview	161
18.2 Status Screen	161
Chapter 19	
Troubleshooting.....	165
19.1 Power, Hardware Connections, and LEDs	165
19.2 MAX-207HW2R Access and Login	166
19.3 Internet Access	168
19.4 Phone Calls and VoIP	170
19.5 Reset the MAX-207HW2R to Its Factory Defaults	171
19.5.1 Pop-up Windows, JavaScripts and Java Permissions	171
Chapter 20	
Product Specifications	173
20.1 Wall-Mounting	180
20.1.1 The Wall-Mounting Kit	180
20.1.2 Instructions	180
Appendix A WiMAX Security	183
Appendix B Setting Up Your Computer's IP Address	187
Appendix C Pop-up Windows, JavaScripts and Java Permissions	215
Appendix D IP Addresses and Subnetting	225
Appendix E Importing Certificates	237
Appendix F SIP Passthrough	269
Appendix G Common Services	271
Appendix H Legal Information	275
Index.....	279

PART I

User's Guide

Getting Started

1.1 About Your MAX-207HW2R

The MAX-207HW2R has a built-in switch and one phone port. It allows you to access the Internet by connecting to a WiMAX wireless network.

You can use a traditional analog telephone to make Internet calls using the MAX-207HW2R's Voice over IP (VoIP) communication capabilities.

You can configure firewall and content filtering as well as a host of other features.

The web browser-based Graphical User Interface (GUI), also known as the web configurator, provides easy management.

See [Chapter 20 on page 173](#) for a complete list of features for your model.

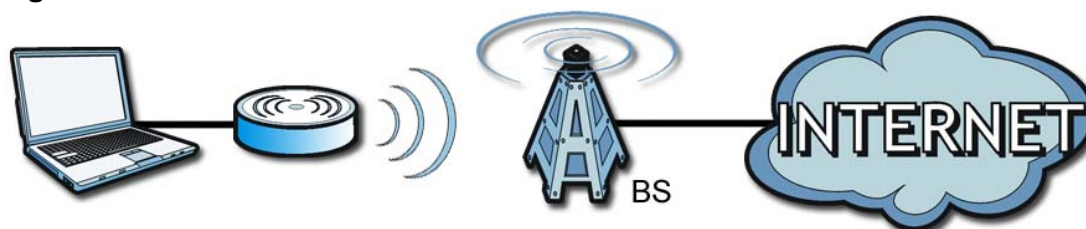
1.1.1 WiMAX Internet Access

Connect your computer or network to the MAX-207HW2R for WiMAX Internet access. See the Quick Start Guide for instructions on hardware connection.

In a wireless metropolitan area network (MAN), the MAX-207HW2R connects to a WiMAX base station (BS) for Internet access.

The following diagram shows a notebook computer equipped with the MAX-207HW2R connecting to the Internet through a WiMAX base station (marked **BS**).

Figure 1 Mobile Station and Base Station



When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network.

Use content filtering to block access to web sites with URLs containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to certain web sites for the kids.

1.1.2 Make Calls via Internet Telephony Service Provider

In a home or small office environment, you can use the MAX-207HW2R to make and receive the following types of VoIP telephone calls:

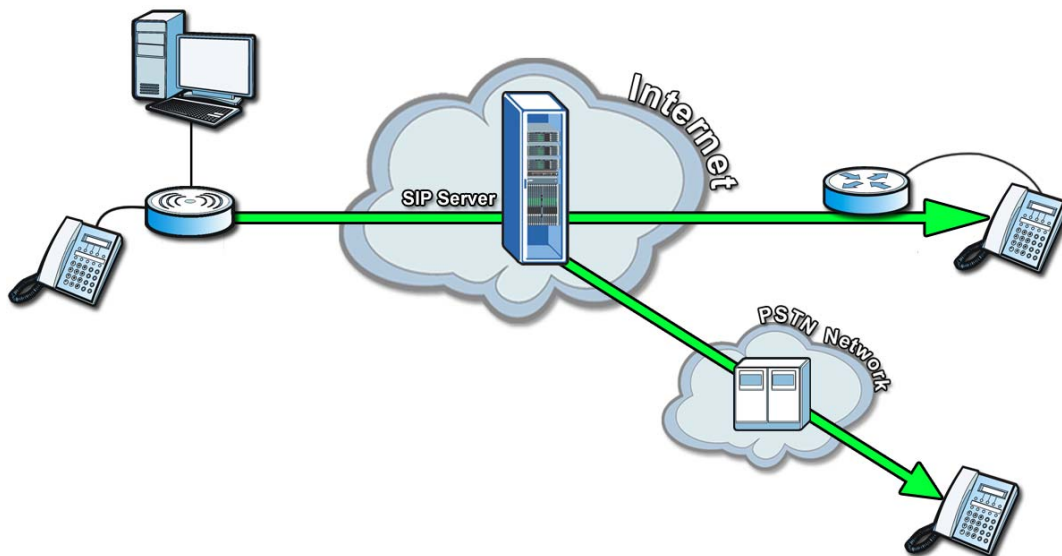
- Peer-to-Peer calls - Use the MAX-207HW2R to make a call directly to the recipient's IP address without using a SIP proxy server.

Figure 2 MAX-207HW2R's VoIP Features - Peer-to-Peer Calls



- Calls via a VoIP service provider - The MAX-207HW2R sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

Figure 3 MAX-207HW2R's VoIP Features - Calls via VoIP Service Provider



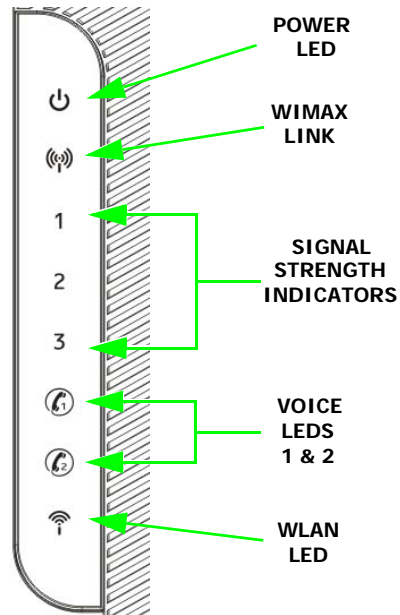
1.2 MAX-207HW2R Hardware

Follow the instructions in the Quick Start Guide to make hardware connections.

1.2.1 LEDs

The following figure shows the LEDs (lights) on the MAX-207HW2R.

Figure 4 The MAX-207HW2R's LEDs



The following table describes your MAX-207HW2R's LEDs (from right to left).

Table 2 The MAX-207HW2R

LED	STATE	DESCRIPTION
Power	Off	The MAX-207HW2R is not receiving power.
	Red	The MAX-207HW2R is receiving power but has been unable to start up correctly or is not receiving enough power. See the Troubleshooting section for more information.
	Green	The MAX-207HW2R is receiving power and functioning correctly.
WiMAX Link	Off	The MAX-207HW2R is not connected to a wireless (WiMAX) network.
	Green	The MAX-207HW2R is successfully connected to a wireless (WiMAX) network.
	Green (Blinking Slowly)	The MAX-207HW2R is searching for a wireless (WiMAX) network.
	Green (Blinking Quickly)	The MAX-207HW2R has found a wireless (WiMAX) network and is connecting.

Table 2 The MAX-207HW2R

LED	STATE	DESCRIPTION
Signal Strength Indicator	The Strength Indicator LEDs display the Interference-plus-Noise Ratio (CINR) of the wireless (WiMAX) connection.	
	Signal 1 On	The signal strength is in the range between 5 and 15.
	Signal 2 On	The signal strength is in the range between 16 and 24.
	Signal 3 On	The signal strength is greater than or equal to 25 dBm
Voice	Off	No SIP account is registered, or the MAX-207HW2R is not receiving power.
	Green	A SIP account is registered.
	Green (Blinking)	A SIP account is registered, and the phone attached to the LINE port is in use (off the hook).
	Yellow	A SIP account is registered and has a voice message on the SIP server.
	Yellow (Blinking)	A SIP account is registered and has a voice message on the SIP server, and the phone attached to the LINE port is in use (off the hook).
WLAN	Off	The Wi-Fi network is not operational.
	Green	The Wi-Fi network is operational.
	Blinking Green	The WiMAX Device is sending and receiving data across the Wi-Fi network.

1.3 Good Habits for Managing the MAX-207HW2R

Do the following things regularly to make the MAX-207HW2R more secure and to manage the MAX-207HW2R more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the MAX-207HW2R becomes unstable or even crashes. If you forget your password, you will have to reset the MAX-207HW2R to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the MAX-207HW2R. You could simply restore your last configuration.

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device set up and management via any web browser that supports: HTML 4.0, CSS 2.0, and JavaScript 1.5, and higher. The recommended screen resolution for using the web configurator is 1024 by 768 pixels and 16-bit color, or higher.

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

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in many operating systems and web browsers.
- JavaScript (enabled by default in most web browsers).
- Java permissions (enabled by default in most web browsers).

See the [Appendix C on page 215](#) for more information on configuring your web browser.

2.1.1 Accessing the Web Configurator

- 1 Make sure your MAX-207HW2R hardware is properly connected (refer to the Quick Start Guide for more information).
- 2 Launch your web browser.
- 3 Enter "192.168.1.1" as the URL.

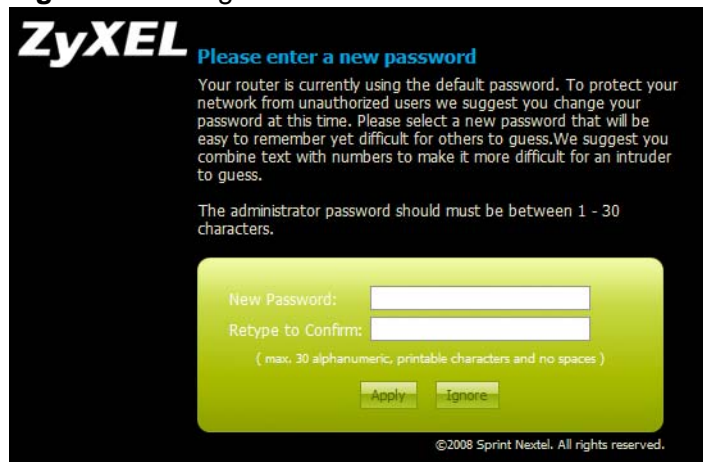
- 4 A login screen displays. Enter the default **User Name** (admin) and **Password** (1234), and then click **Login**.

Figure 5 Password Screen



- 5 The following screen displays if you have not yet changed your password. It is highly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 6 Change Password Screen



2.1.2 The Reset Button

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

2.1.2.1 Using The Reset Button

- 1 Make sure the **Power** light is on (not blinking).

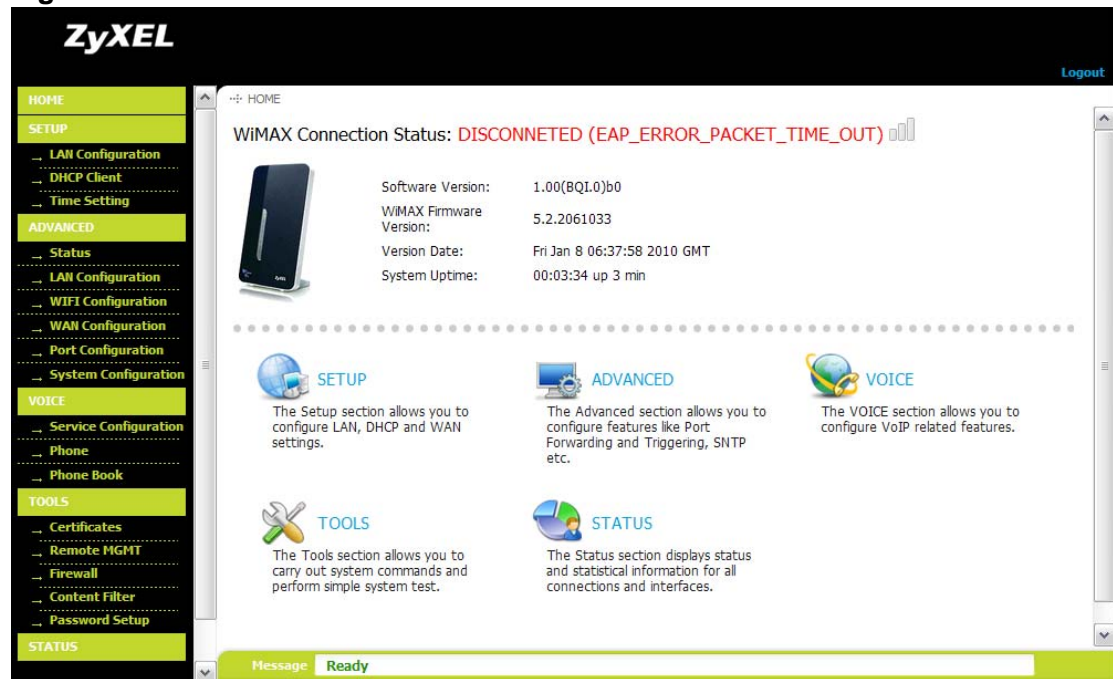
- 2 To set the device back to the factory default settings, press the **Reset** button for ten seconds or until the **Power** light begins to blink and then release it. When the **Power** light begins to blink, the defaults have been restored and the device restarts.
- 3 Reconfigure the MAX-207HW2R following the steps in your Quick Start Guide.

2.2 The Main Screen

When you first log into the web configurator and by-pass the wizard, the Main screen appears. Here you can view a concise summary of your MAX-207HW2R connection status. This is also the default “home” page for the ZyXEL web configurator and it contains conveniently-placed shortcuts to all of the other screens.







Note: Some features in the web configurator may not be available depending on your firmware version and/or configuration.

Figure 7 Main Screen



The following table describes the icons in this screen.

Table 3 Main > Icons

ICON	DESCRIPTION
	<p>SETUP</p> <p>Click to go the Setup screen, where you can configure LAN, DHCP and WAN settings.</p>
	<p>ADVANCED</p> <p>Click to go to the Advanced screen, where you can configure features like Port Forwarding and Triggering, SNTP and so on.</p>
	<p>VOICE</p> <p>Click to go to the Voice screen, where you can configure your voice service and phone settings.</p>
	<p>TOOLS</p> <p>Click to go the Tools screen, where you can configure your firewall, QoS, and content filter, among other things.</p>
	<p>STATUS</p> <p>Click to go to the Status screen, where you can view status and statistical information for all connections and interfaces.</p>
	<p>Strength Indicator</p> <p>Displays a visual representation of the quality of your WIMAX connection.</p> <ul style="list-style-type: none"> • Disconnected - Zero bars • Poor reception - One bar • Good reception - Two bars • Excellent reception - Three bars

The following table describes the labels in this screen.

Table 4 Main

LABEL	DESCRIPTION
Logout	<p>Click to log out of the Web Configurator.</p> <p>Note: This does not log you off the WiMAX network, it simply logs you out of the MAX-207HW2R's browser-based configuration interface.</p>
WiMAX Connection Status	<p>This field indicates the current status of your WiMAX connection.</p> <p>Status messages are as follows:</p> <ul style="list-style-type: none"> • Connected - Indicates that the MAX-207HW2R is connected to the WiMAX network. Use the Strength Indicator icon to determine the quality of your network connection. • Disconnected - Indicates that the MAX-207HW2R is not connected to the WiMAX network. • DL_SYN - Indicates a download synchronization is in progress. This means the firmware is checking with the server for any updates or settings alterations.
Software Version	<p>This field indicates the version number of the MAX-207HW2R's firmware. The version number takes the form of: <i>Version (Build), release status (candidate) Version Release Date</i>.</p> <p>For example: V3.60(BCC.0)c4 07/08/2008 indicates that the firmware is 3.60, build BCC.0, candidate4, released on July 08, 2008.</p>
WiMAX Firmware Version	This field displays the version number of the chip firmware used in this MAX-207HW2R.
Version Date	This field indicates the exact date and time the current firmware was compiled.
System Uptime	This field indicates how long the MAX-207HW2R has been on. This resets every time you shut the device down or restart it.

Note: For security reasons, the MAX-207HW2R automatically logs you out if you do not use the web configurator for five minutes. If this happens, simply log in again.

PART II

Technical Reference

The Setup Screens

3.1 Overview

Use these screens to configure or view LAN, DHCP Client and WAN settings.

3.1.1 What You Can Do in This Chapter

- The **LAN Configuration** screen ([Section 3.2 on page 32](#)) lets you configure the MAX-207HW2R's IP address and subnet mask.
- The **DHCP Client** screen ([Section 3.3 on page 33](#)) lets you view all DHCP client information.
- The **Time Setting** screen ([Section 3.4 on page 35](#)) lets you configure your MAX-207HW2R's time and date keeping settings.

3.1.2 What You Need to Know

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

LAN

A Local Area Network, or a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area such as a home or office environment. LANs have different topologies, the most common being the linear bus and the star configuration.

IP Address

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

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP Address that

you entered. You do not need to change the computer subnet mask unless you are instructed to do so.

DHCP

Your WiMAX Modem can act as a DHCP (Dynamic Host Configuration Protocol) server that can assign your LAN computers an IP address, subnet mask, DNS and other routing information when its LAN DHCP feature is turned on.

Daytime

A network protocol used by devices for debugging and time measurement. A computer can use this protocol to set its internal clock but only if it knows in which order the year, month, and day are returned by the server. Not all servers use the same format.

Time

A network protocol for retrieving the current time from a server. The computer issuing the command compares the time on its clock to the information returned by the server, adjusts itself automatically for time zone differences, then calculates the difference and corrects itself if there has been any temporal drift.

NTP

NTP stands for Network Time Protocol. It is employed by devices connected to the Internet in order to obtain a precise time setting from an official time server. These time servers are accurate to within 200 microseconds.

3.1.3 Before You Begin

- Make sure that you have made all the appropriate hardware connections to the MAX-207HW2R, as described in the Quick Start Guide.
- Make sure that you have logged in to the web configurator at least one time and changed your password from the default, as described in the Quick Start Guide.

3.2 LAN Configuration

Click the **SETUP** icon in the navigation bar to set up the MAX-207HW2R's IP address and subnet mask. This screen displays this screen by default. If you are in

any other sub-screen you can simply choose **Set IP Address** from the navigation menu on the left to open it again.

Figure 8 SETUP > Set IP Address

LAN IP Configuration

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

Apply Reset

The following table describes the labels in this screen.

Table 5 SETUP > Set IP Address

LABEL	DESCRIPTION
IP Address	Enter the IP address of the MAX-207HW2R on the LAN. Note: This field is the IP address you use to access the MAX-207HW2R on the LAN. If the web configurator is running on a computer on the LAN, you lose access to it as soon as you change this field and click Apply . You can access the web configurator again by typing the new IP address in the browser.
IP Subnet Mask	Enter the subnet mask of the LAN.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

3.3 DHCP Client

Click **SETUP > DHCP Client** to display the IP addresses, Host Names and MAC addresses of the devices currently connected to the MAX-207HW2R. These

settings can be configured in the **ADVANCED > LAN Configuration > DHCP Setup** screen.

Figure 9 SETUP > DHCP Client

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.58	twpc13774-02	00:24:21:7e:20:96	<input type="checkbox"/>
2	192.168.1.33	twpc11947-01	00:19:cb:32:be:ac	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 6 SETUP > DHCP Client

LABEL	DESCRIPTION
#	The number of the item in this list.
IP Address	This field displays the IP address the MAX-207HW2R assigned to a computer in the network.
Host Name	This field displays the system name of the computer to which the MAX-207HW2R assigned the IP address.
MAC Address	This field displays the MAC address of the computer to which the MAX-207HW2R assigned the IP address.
Reserve	Select Reserve and click Apply to have the MAX-207HW2R always map the currently assigned IP address to the device with this MAC address.
Apply	Clear Reserve and click Apply to allow the MAX-207HW2R to assign a new IP address to this device with this MAC address when next time the device sends a new DHCP request.
Refresh	Click this button to update the table data.

3.4 Time Setting

Click **SETUP > Time Setting** to set the date, time, and time zone for the MAX-207HW2R.

Figure 10 SETUP > Time Setting

The following table describes the labels in this screen.

Table 7 SETUP > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	Displays the current time according to the MAX-207HW2R.
Current Date	Displays the current time according to the MAX-207HW2R.
Time and Date Setup	
Manual	Select this if you want to specify the current date and time in the fields below.
New Time	Enter the new time in this field, and click Apply .
New Date	Enter the new date in this field, and click Apply .
Get from Time Server	Select this if you want to use a time server to update the current date and time in the MAX-207HW2R.

Table 7 SETUP > Time Setting

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server uses. Check with your ISP or network administrator, or use trial-and-error to find a protocol that works. Daytime (RFC 867) - This format is day/month/year/time zone. Time (RFC 868) - This format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC 1305) - This format is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Select the time zone at your location.
Daylight Savings	Select this if your location uses daylight savings time. Daylight savings is a period from late spring to early fall when many places set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter which hour on which day of which week of which month daylight-savings time starts.
End Date	Enter which hour on the which day of which week of which month daylight-savings time ends.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

3.4.1 Pre-Defined NTP Time Servers List

The MAX-207HW2R uses a pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified. It can use this list regardless of the time protocol you select.

When the MAX-207HW2R uses the list, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then it goes through the rest of the list in order until either it is successful or all the pre-defined NTP time servers have been tried.

Table 8 Pre-defined NTP Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se

Table 8 Pre-defined NTP Time Servers (continued)

time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

3.4.2 Resetting the Time

The MAX-207HW2R automatically resets the time in the following circumstances:

- When the device starts up, such as when you press the **Power** button.
- When you click **Apply** in the **SETUP > Time Setting** screen.
- Once every 24-hours after starting up.

The Status Screen

4.1 Overview

Use this screen to view a complete summary of your MAX-207HW2R connection status.

4.2 Status Screen

Click **Advanced** > **STATUS** in the navigation bar to go to this screen, where you can view the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and un-register SIP accounts as well as view detailed information from DHCP and statistics from WiMAX, VoIP, bandwidth management, and traffic.

Figure 11 Advanced > Status

The screenshot shows the 'Advanced > Status' screen. At the top right, there is a 'Refresh Interval' dropdown menu set to 'None' and a 'Refresh Now' button. The screen is divided into three main sections: Device Information, Interface Status, and WiMAX Information.

Device Information	
System Name:	MAX-207HW2
Software Version:	1.00(BQI.0)b0
Bootbase Version:	1.09
Kernel Version:	2.6.21.1
WAN Information:	
IP Address:	
IP Subnet Mask:	
DHCP:	Client
LAN Information:	
IP Address:	192.168.1.1
IP Subnet Mask:	255.255.255.0
DHCP:	Server
WiMAX Information	
CINR Mean:	24 dB
CINR Deviation:	0 dB
RSSI:	-60 dBm

Interface Status	
Interface	Status
WAN	Down
LAN	Up

The following tables describe the labels in this screen.

Table 9 Advanced > Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the MAX-207HW2R to update this screen.
Refresh Now	Click this to update this screen immediately.

Table 9 Advanced > Status (continued)

LABEL	DESCRIPTION
Device Information	
System Name	This field displays the MAX-207HW2R system name. It is used for identification.
Software Version	This field displays the current firmware version inside the device. You can change the firmware version by uploading new firmware in ADVANCED > System Configuration > Firmware .
Bootbase Version	This field displays the current bootbase version inside the device.
Kernel Version	This field displays the current kernel version inside the device.
WAN Information	
IP Address	This field displays the current IP address of the MAX-207HW2R in the WAN.
IP Subnet Mask	This field displays the current subnet mask on the WAN.
DHCP	This field displays what DHCP services the MAX-207HW2R is using in the WAN. Choices are: Client - The MAX-207HW2R is a DHCP client in the WAN. Its IP address comes from a DHCP server on the WAN. None - The MAX-207HW2R is not using any DHCP services in the WAN. It has a static IP address.
LAN Information	
IP Address	This field displays the current IP address of the MAX-207HW2R in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the MAX-207HW2R is providing to the LAN. Choices are: Server - The MAX-207HW2R is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The MAX-207HW2R is routing DHCP requests to one or more DHCP servers. The DHCP server(s) may be on another network. None - The MAX-207HW2R is not providing any DHCP services to the LAN. You can change this in ADVANCED > LAN Configuration > DHCP Setup .
WiMAX Information	
CINR Mean	This field shows the average Carrier to Interference plus Noise Ratio of the current connection. This value is an indication of overall radio signal quality. A higher value indicates a higher signal quality, and a lower value indicates a lower signal quality.
CINR Deviation	This field shows the amount of change in the CINR level. This value is an indication of radio signal stability. A lower number indicates a more stable signal, and a higher number indicates a less stable signal.

Table 9 Advanced > Status (continued)

LABEL	DESCRIPTION
RSSI	<p>This field shows the Received Signal Strength Indication. This value is a measurement of overall radio signal strength. A higher RSSI level indicates a stronger signal, and a lower RSSI level indicates a weaker signal.</p> <p>A strong signal does not necessarily indicate a good signal: a strong signal may have a low signal-to-noise ratio (SNR).</p>
Interface Status	
Interface	This column displays each interface of the MAX-207HW2R.
Status	<p>This field indicates whether or not the MAX-207HW2R is using the interface.</p> <p>For the WAN interface, this field displays Up when the MAX-207HW2R is connected to a WiMAX network, and Down when the MAX-207HW2R is not connected to a WiMAX network.</p> <p>For the LAN interface, this field displays Up when the MAX-207HW2R is using the interface and Down when the MAX-207HW2R is not using the interface.</p>

The LAN Configuration Screens

5.1 Overview

Use the **ADVANCED > LAN Configuration** screens to set up the MAX-207HW2R on the LAN. You can configure its IP address and subnet mask, DHCP services, and other subnets. You can also control how the MAX-207HW2R sends routing information using RIP.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually a computer network limited to the immediate area, such as the same building or floor of a building.

5.1.1 What You Can Do in This Chapter

- The **DHCP Setup** screen ([Section 5.2 on page 44](#)) lets you enable, disable, and configure the DHCP server in the MAX-207HW2R.
- The **Static DHCP** screen ([Section 5.3 on page 45](#)) lets you assign specific IP addresses to specific computers on the LAN.
- The **IP Alias** screen ([Section 5.4 on page 47](#)) lets you add subnets on the LAN port. You can also control what routing information is sent and received by each subnet.
- The **Advanced** screen ([Section 5.5 on page 49](#)) lets you control the routing information that is sent and received by each subnet assign specific IP addresses to specific computers on the LAN.

5.1.2 What You Need to Know

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

IP Address

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

Subnet Masks

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

DNS

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

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your MAX-207HW2R an IP address, subnet mask, DNS and other routing information when it's turned on.

5.2 DHCP Setup

Click **ADVANCED > LAN Configuration > DHCP Setup** to enable, disable, and configure the DHCP server in the MAX-207HW2R.

Figure 12 ADVANCED > LAN Configuration > DHCP Setup

The screenshot shows the DHCP Setup configuration page. At the top, there are four tabs: DHCP Setup, Static DHCP, IP Alias, and Advanced. The DHCP Setup tab is selected. Below the tabs, there are two main sections: DHCP Setup and DNS Server. In the DHCP Setup section, the 'Enable DHCP Server' checkbox is checked. The 'IP Pool Starting Address' is set to 192.168.1.33, the 'lease time(second)' is 86400, and the 'Pool Size' is 32. In the DNS Server section, there are three rows for 'DNS Servers Assigned by DHCP Server'. Each row has a dropdown menu set to 'From ISP' and a text input field containing '0.0.0.0'. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 10 ADVANCED > LAN Configuration > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
Enable DHCP Server	Select this if you want the MAX-207HW2R to be the DHCP server on the LAN. As a DHCP server, the MAX-207HW2R assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information.
IP Pool Starting Address	Enter the IP address from which the MAX-207HW2R begins allocating IP addresses, if you have not specified an IP address for this computer in ADVANCED > LAN Configuration > Static DHCP .
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by a subnet mask of 255.255.255.0 (regardless of the subnet the MAX-207HW2R is in). For example, if the IP Pool Start Address is 10.10.10.10, the MAX-207HW2R can allocate up to 10.10.10.254, or 245 IP addresses.
lease time (second)	You can assign the DHCP lease time by entering the seconds manually. The lease time must be 120 seconds or more.
DNS Server	
First, Second and Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. The MAX-207HW2R provides these IP addresses to DHCP clients. You can specify these IP addresses two ways. From ISP - provide the DNS servers provided by the ISP on the WAN port. User Defined - enter a static IP address. DNS Relay - this setting will relay DNS information from the DNS server obtained by the MAX-207HW2R. None - no DNS service will be provided by the MAX-207HW2R.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

5.3 Static DHCP

Click **ADVANCED > LAN Configuration > Static DHCP** to assign specific IP addresses to specific computers on the LAN.

Note: This screen has no effect if the DHCP server is not enabled. You can enable it in **ADVANCED > LAN Configuration > DHCP Setup**.

Figure 13 ADVANCED > LAN Configuration > Static DHCP

#	MAC Address	IP Address
1	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>
2	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>
3	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>
4	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>
5	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>
6	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>
7	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>
8	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0.0.0.0"/>

The following table describes the labels in this screen.

Table 11 ADVANCED > LAN Configuration > Static DHCP

LABEL	DESCRIPTION
#	The number of the item in this list.
MAC Address	Enter the MAC address of the computer to which you want the MAX-207HW2R to assign the same IP address.
IP Address	Enter the IP address you want the MAX-207HW2R to assign to the computer.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

5.4 IP Alias

Click **ADVANCED > LAN Configuration > IP Alias** to add subnets on the LAN port. You can also control what routing information is sent and received by each subnet.

Figure 14 ADVANCED > LAN Configuration > IP Alias

The screenshot shows the 'IP Alias' configuration page. It has tabs for 'DHCP Setup', 'Static DHCP', 'IP Alias', and 'Advanced'. Under 'IP Alias 1', there is a checkbox 'IP Alias 1', an 'IP Address' field, an 'IP Subnet Mask' field, a 'RIP Direction' dropdown menu (set to 'None'), and a 'RIP Version' dropdown menu (set to 'RIP-1'). A similar section exists for 'IP Alias 2'. At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 12 ADVANCED > LAN Configuration > IP Alias

LABEL	DESCRIPTION
IP Alias 1	
IP Alias 1	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the MAX-207HW2R on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the MAX-207HW2R sends and receives on the subnet. <ul style="list-style-type: none"> • None - The MAX-207HW2R does not send or receive routing information on the subnet. • Both - The MAX-207HW2R sends and receives routing information on the subnet. • In Only - The MAX-207HW2R only receives routing information on the subnet. • Out Only - The MAX-207HW2R only sends routing information on the subnet.

Table 12 ADVANCED > LAN Configuration > IP Alias (continued)

LABEL	DESCRIPTION
RIP Version	Select which version of RIP the MAX-207HW2R uses when it sends or receives information on the subnet. <ul style="list-style-type: none"> • RIP-1 - The MAX-207HW2R uses RIPv1 to exchange routing information. • RIP-2B - The MAX-207HW2R broadcasts RIPv2 to exchange routing information. • RIP-2M - The MAX-207HW2R multicasts RIPv2 to exchange routing information.
IP Alias 2	
IP Alias 2	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the MAX-207HW2R on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the MAX-207HW2R sends and receives on the subnet. <ul style="list-style-type: none"> • None - The MAX-207HW2R does not send or receive routing information on the subnet. • Both - The MAX-207HW2R sends and receives routing information on the subnet. • In Only - The MAX-207HW2R only receives routing information on the subnet. • Out Only - The MAX-207HW2R only sends routing information on the subnet.
RIP Version	Select which version of RIP the MAX-207HW2R uses when it sends or receives information on the subnet. <ul style="list-style-type: none"> • RIP-1 - The MAX-207HW2R uses RIPv1 to exchange routing information. • RIP-2B - The MAX-207HW2R broadcasts RIPv2 to exchange routing information. • RIP-2M - The MAX-207HW2R multicasts RIPv2 to exchange routing information.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

5.5 Advanced

Click **ADVANCED > LAN Configuration > Advanced** to set the RIP and Multicast options.

Figure 15 ADVANCED > LAN Configuration > Advanced

The screenshot shows a web interface for configuring network settings. At the top, there are tabs for 'DHCP Setup', 'Static DHCP', 'IP Alias', and 'Advanced'. The 'Advanced' tab is selected. Below the tabs is a section titled 'RIP & Multicast Setup' with a dashed border. Inside this section, there are three labels with corresponding dropdown menus: 'RIP Direction:' set to 'None', 'RIP Version:' set to 'RIP-1', and 'Multicast:' set to 'None'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 13 ADVANCED > LAN Configuration > Advanced

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	<p>Use this field to control how much routing information the MAX-207HW2R sends and receives on the subnet.</p> <ul style="list-style-type: none"> • None - The MAX-207HW2R does not send or receive routing information on the subnet. • Both - The MAX-207HW2R sends and receives routing information on the subnet. • In Only - The MAX-207HW2R only receives routing information on the subnet. • Out Only - The MAX-207HW2R only sends routing information on the subnet.
RIP Version	<p>Select which version of RIP the MAX-207HW2R uses when it sends or receives information on the subnet.</p> <ul style="list-style-type: none"> • RIP-1 - The MAX-207HW2R uses RIPv1 to exchange routing information. • RIP-2B - The MAX-207HW2R broadcasts RIPv2 to exchange routing information. • RIP-2M - The MAX-207HW2R multicasts RIPv2 to exchange routing information.

Table 13 ADVANCED > LAN Configuration > Advanced (continued)

LABEL	DESCRIPTION
Multicast	<p>You do not have to enable multicasting to use RIP-2M. (See RIP Version.)</p> <p>Select which version of IGMP the MAX-207HW2R uses to support multicasting on the LAN. Multicasting sends packets to some computers on the LAN and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer).</p> <ul style="list-style-type: none"> • None - The MAX-207HW2R does not support multicasting. • IGMP-v1 - The MAX-207HW2R supports IGMP version 1. • IGMP-v2 - The MAX-207HW2R supports IGMP version 2. <p>Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the LAN have to support the same version of IGMP.</p>
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

5.6 Technical Reference

The following section contains additional technical information about the MAX-207HW2R features described in this chapter.

5.6.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the MAX-207HW2R. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.100.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.100.1, for your MAX-207HW2R, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your MAX-207HW2R will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the MAX-207HW2R unless you are instructed to do otherwise.

5.6.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the MAX-207HW2R as a DHCP server or disable it. When configured as a server, the MAX-207HW2R provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else each computer must be manually configured.

The MAX-207HW2R is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see [Section 5.3 on page 45](#).

5.6.3 LAN TCP/IP

The MAX-207HW2R has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

The LAN parameters of the MAX-207HW2R are preset in the factory with the following values:

- IP address of 192.168.100.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see [Section 5.3 on page 45](#).

5.6.4 DNS Server Address

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

The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISPs choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The MAX-207HW2R supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in the **LAN Setup** screen are not specified, for instance, left as 0.0.0.0, the MAX-207HW2R tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the MAX-207HW2R, the MAX-207HW2R forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen. This way, the MAX-207HW2R can pass the DNS servers to the computers and the computers can query the DNS server directly without the MAX-207HW2R's intervention.

5.6.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the MAX-207HW2R will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the MAX-207HW2R will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the MAX-207HW2R will send out RIP packets but will not accept any RIP packets received.
- **None** - the MAX-207HW2R will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the MAX-207HW2R sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information.

RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

5.6.6 Multicast

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

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

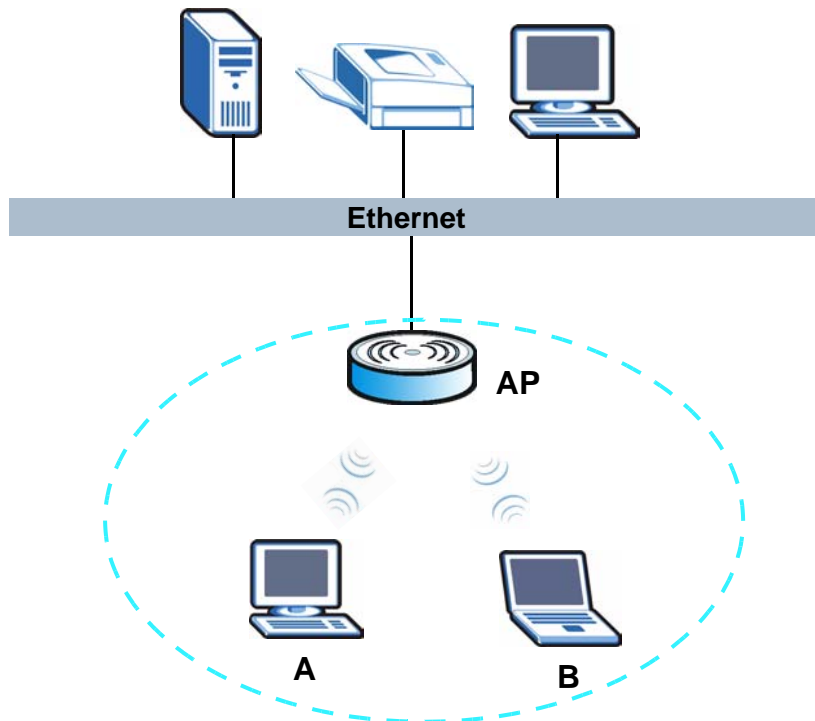
The MAX-207HW2R supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the MAX-207HW2R queries all directly connected networks to gather group membership. After that, the MAX-207HW2R periodically updates this information. IP multicasting can be enabled/disabled on the MAX-207HW2R LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

The WIFI Configuration Screen

6.1 Overview

Wi-Fi is a wireless networking technology and it is a synonym for wireless LAN. The blue circle marks a wireless LAN in the following figure. Wireless clients (A and B) connect to an access point (AP) to access other devices (such as the printer) or the Internet. Your MAX-207HW2R works as an AP when you install a compatible WLAN card.

Figure 16 Example of a Wireless Network



6.1.1 What You Can Do in the WIFI Screens

This chapter describes the MAX-207HW2R's **Advanced > WIFI Configuration** screens. Use these screens to set up your MAX-207HW2R's wireless connection.

- Use the **General** screen (see [Section 6.2 on page 59](#)) to turn the wireless connection on or off, set up wireless security, configure the MAC filter, set up Quality of Service and make other basic configuration changes.
- Use the **MAC Filter** screen (see [Section 6.3 on page 64](#)) to configure a MAC (Media Access Control) address filter to restrict access to the wireless network.
- Use the **WPS** screen (see [Section 6.4 on page 65](#)) to set up WPS by pressing a button or using a PIN.

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

6.1.2 What You Need to Know About WIFI

Wireless Basics

- Every device in the same wireless network must use the same Service Set IDentity (SSID).
The SSID is the name of the wireless network.
- If two wireless networks overlap, they should use different channels.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

Wireless Network Construction

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

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

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

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

Wired Equivalent Privacy (WEP)

WEP (Wired Equivalent Privacy) encrypts data transmitted between wired and wireless networks to keep the transmission private. Although one of the original wireless encryption protocols, WEP is also the weakest. Many people use it strictly to deter unintentional usage of their wireless network by outsiders.

Authentication Type

The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Three authentication types are defined: **Auto**, **Open** and **Shared**. The MAX-207HW2R supports the **WEP (Open)** and **WEP (Shared)** authentication types.

- **Open** mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- **Shared** mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

Wi-Fi Protected Access (WPA)

WPA encrypts data transmitted between wired and wireless networks to keep the transmission private. It affords vastly stronger security than its lower-tier counterpart, WEP (Wired Equivalent Privacy). It comes in two different flavors: WPA and WPA2. Always try to use WPA2 as it implements the full version of the security standard while WPA does not.

WPA2

WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It includes two data encryption algorithms, Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication Code Protocol (CCMP). WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be implemented in all wireless devices. See also WPA.


Pre-Shared Key (PSK)

A pre-shared key is a password shared between the server and the client that unlocks the algorithm used to encrypt the data traffic between them. Without the proper password, the client and the server cannot communicate.

Security

Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network. Use the strongest security that every wireless client in the wireless network supports.

Table 14 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Weakest  Strongest	No Security
	MAC Filter
	WEP Encryption
	IEEE 802.1x EAP with RADIUS Server Authentication
	WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)
	WPA (Wi-Fi Protected Access)
	WPA-PSK2
	WPA2

Note: WPA2 or WPA2-PSK security is recommended.

- WPA2-PSK and WPA-PSK do not employ user authentication and are known as the personal version of WPA.
- WEP is better than no security, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

MAC Filter

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address consists of twelve hexadecimal characters (0-9, and A to F), and it is usually written in the following format: "0A:A0:00:BB:CC:DD".

The MAC filter controls access to the wireless network. You can use the MAC address of each wireless client to allow or deny access to the wireless network.

Finding Out More

- See [Section 6.5 on page 66](#) for advanced technical information on wireless networks.

6.1.3 Before You Start

Before you start using these screens, ask yourself the following questions. See [Section 6.1.2 on page 56](#) if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

6.2 General Screen

Note: If you are configuring the MAX-207HW2R from a computer connected to the wireless LAN and you change the MAX-207HW2R's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the MAX-207HW2R's new settings.

Click **Advanced > WIFI Configuration** to open the **General** screen.

Figure 17 Advanced > WIFI Configuration > General

The screenshot displays the 'General' configuration screen for the MAX-207HW2R. It features three tabs: 'General', 'MAC Filter', and 'WPS'. The 'General' tab is active. The 'Wireless Setup' section includes a checked 'Active Wireless LAN' checkbox, a text field for 'Network Name(SSID)' containing 'ZyXEL', an unchecked 'Hide SSID' checkbox, and a dropdown menu for 'Channel Selection' set to 'Channel-01 2412MHZ'. The 'Security' section has a dropdown menu for 'Security Mode' set to 'No Security'. At the bottom of the screen, there are three buttons: 'Apply', 'Reset', and 'Advanced Setup'.

The following table describes the labels in this screen.

Table 15 Advanced > WIFI Configuration > General

LABEL	DESCRIPTION
Wireless Setup	
Active Wireless LAN	Click the check box to activate wireless LAN.
Network Name (SSID)	<p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <p>Note: If you are configuring the MAX-207HW2R from a computer connected to the wireless LAN and you change the MAX-207HW2R's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the MAX-207HW2R's new settings.</p>
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Security	
Channel Selection	Select this option and set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Security Mode	See the following sections for more details about this field.
Apply	Click Apply to save your changes back to the MAX-207HW2R.
Reset	Click to restore your previously saved settings.
Advanced Setup	Click Advanced Setup to display the Wireless Advanced Setup screen and edit more details of your WLAN setup.

6.2.1 No Security

Select **No Security** in the **Security Mode** field to allow wireless devices to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your MAX-207HW2R, your network is accessible to any wireless networking device that is within range.

Figure 18 Advanced > WIFI Configuration > General: No Security

The screenshot shows the 'General' tab of the 'WIFI Configuration' screen. Under 'Wireless Setup', the 'Active Wireless LAN' checkbox is checked. The 'Network Name (SSID)' field contains 'ZyXEL'. The 'Hide SSID' checkbox is unchecked. The 'Channel Selection' dropdown is set to 'Channel-01 2412MHZ'. Under the 'Security' section, the 'Security Mode' dropdown is set to 'No Security'. At the bottom, there are three buttons: 'Apply', 'Reset', and 'Advanced Setup'.

6.2.2 WEP Encryption

In order to configure and enable WEP encryption; click **Advanced > WIFI Configuration > General** to display the **General** screen. Select **WEP (OPEN)** or **WEP (SHARED)** from the **Security Mode** list.

Figure 19 Advanced > WIFI Configuration > General: WEP (OPEN) / WEP (SHARED)

The screenshot shows the 'General' tab of the 'WIFI Configuration' screen. Under 'Wireless Setup', the 'Active Wireless LAN' checkbox is checked. The 'Network Name (SSID)' field contains 'ZyXEL'. The 'Hide SSID' checkbox is unchecked. The 'Channel Selection' dropdown is set to 'Channel-01 2412MHZ'. Under the 'Security' section, the 'Security Mode' dropdown is set to 'WEP (OPEN)'. Below this is a 'WEP Key' input field. A 'NOTE' section contains the following text: 'NOTE: The different WEP lengths configure different strength security, 40/64-bit or 128-bit respectively. Your wireless client must match the security strength set on the router. --Please type exactly 5 or 13 characters.' At the bottom, there are three buttons: 'Apply', 'Reset', and 'Advanced Setup'.

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

Table 16 Advanced > WIFI Configuration > General: WEP (OPEN) / WEP (SHARED)

LABEL	DESCRIPTION
Security Mode	Choose WEP (OPEN) or WEP (SHARED) from the drop-down list box.
WEP Key	The WEP key is used to encrypt data. Both the MAX-207HW2R and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.

6.2.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Advanced > WIFI Configuration** to display the **General** screen. Select **WPA-PSK (AES)**, **WPA2-PSK (AES)**, **WPA-PSK (TKIP)**, or **WPA2-PSK (TKIP)** from the **Security Mode** list.

Figure 20 Advanced > WIFI Configuration > General: WPA(2)-PSK (AES/TKIP)

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

Table 17 Advanced > WIFI Configuration > General: WPA(2)-PSK (AES/TKIP)

LABEL	DESCRIPTION
Security Mode	Choose WPA-PSK (AES) , WPA2-PSK (AES) , WPA-PSK (TKIP) , or WPA2-PSK (TKIP) from the drop-down list box.
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

6.2.4 Wireless LAN Advanced Setup

To configure advanced wireless settings, click the **Advanced Setup** button in the **General** screen. The screen appears as shown.

Figure 21 Advanced > WIFI Configuration > General > Advanced Setup

The following table describes the labels in this screen.

Table 18 Advanced > WIFI Configuration > General > Advanced Setup

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 1 and 2347.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Preamble	Select a preamble type. Choices are Long , or Short . The default setting is Long . See the appendix for more information.
802.11 Mode	Select 802.11B/G mixed to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the MAX-207HW2R. Select 802.11B only to allow only IEEE 802.11b compliant WLAN devices to associate with the MAX-207HW2R. Select 802.11A only to allow only IEEE 802.11a compliant WLAN devices to associate with the MAX-207HW2R. Select 802.11G only to allow only IEEE 802.11g compliant WLAN devices to associate with the MAX-207HW2R.
Apply	Click Apply to save your changes back to the MAX-207HW2R.
Reset	Click to restore your previously saved settings.
Back	Click this to return to the previous screen without saving changes.

6.3 MAC Filter

Use this screen to change your MAX-207HW2R's MAC filter settings. Click **Advanced > WIFI Configuration > MAC Filter**. The screen appears as shown.

Figure 22 Advanced > WIFI Configuration > MAC Filter

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:00	10	00:00:00:00:00:00
11	00:00:00:00:00:00	12	00:00:00:00:00:00
13	00:00:00:00:00:00	14	00:00:00:00:00:00
15	00:00:00:00:00:00	16	00:00:00:00:00:00
17	00:00:00:00:00:00	18	00:00:00:00:00:00
19	00:00:00:00:00:00	20	00:00:00:00:00:00
21	00:00:00:00:00:00	22	00:00:00:00:00:00
23	00:00:00:00:00:00	24	00:00:00:00:00:00
25	00:00:00:00:00:00	26	00:00:00:00:00:00
27	00:00:00:00:00:00	28	00:00:00:00:00:00
29	00:00:00:00:00:00	30	00:00:00:00:00:00
31	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 19 Advanced > WIFI Configuration > MAC Filter

LABEL	DESCRIPTION
Active MAC Filter	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Address table. Select Allow to permit access to the MAX-207HW2R, MAC addresses not listed will be denied access to the MAX-207HW2R. Select Deny to block access to the MAX-207HW2R, MAC addresses not listed will be allowed to access the MAX-207HW2R.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the MAX-207HW2R in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

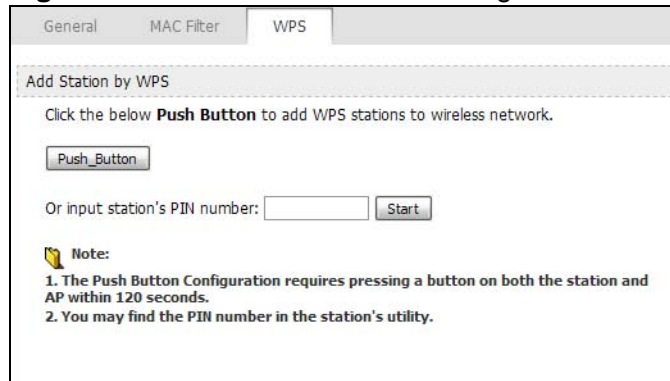
Table 19 Advanced > WIFI Configuration > MAC Filter

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the MAX-207HW2R.
Reset	Click to restore your previously saved settings.

6.4 WPS

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Click **ADVANCED > WIFI Configuration > WPS**. The following screen displays.

Figure 23 ADVANCED > WIFI Configuration > WPS

The following table describes the labels in this screen.

Table 20 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Add Station by WPS	
Push Button	Click this to add another WPS-enabled wireless device (within wireless range of the MAX-207HW2R) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the Push Button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Or input station's PIN number	Enter the PIN of the device that you are setting up a WPS connection with and click Start to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the MAX-207HW2R.

6.5 Wireless LAN Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

6.5.1 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the MAX-207HW2R's Web Configurator.

Table 21 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the MAX-207HW2R. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the MAX-207HW2R.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the MAX-207HW2R does, it cannot communicate with the MAX-207HW2R.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

6.5.2 Wireless Security Overview

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

6.5.2.1 Network Name (SSID)

Normally, the MAX-207HW2R acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the MAX-207HW2R does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

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

6.5.2.2 MAC Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the MAX-207HW2R which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

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

6.5.2.3 User Authentication

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

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

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

6.5.2.4 Encryption

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

-
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of authentication. (See [Section 6.5.2.3](#) on page 67 for information about this.)

Table 22 Types of Encryption for Each Type of Authentication

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

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

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the MAX-207HW2R and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

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

When you select **WPA2** or **WPA2-PSK** in your MAX-207HW2R, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the MAX-207HW2R.

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

6.5.3 WiFi Protected Setup

Your MAX-207HW2R supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works

between two devices. Both devices must support WPS (check each device's documentation to make sure).

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

6.5.3.1 Push Button Configuration

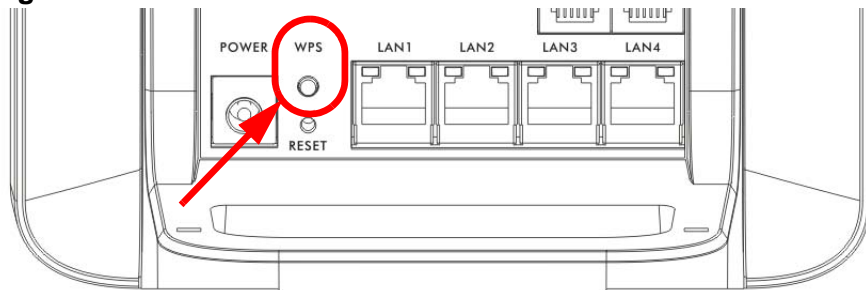
WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

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

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

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this). The MAX-207HW2R's **WPS** button is in the rear panel as shown next.

Figure 24 The WPS Button on the MAX-207HW2R



- 3 Press the button on one of the devices (it doesn't matter which). For the MAX-207HW2R you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

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

The WAN Configuration Screens

7.1 Overview

Use the **ADVANCED > WAN Configuration** screens to set up your MAX-207HW2R's Wide Area Network (WAN) or Internet features.

A Wide Area Network (or WAN) links geographically dispersed locations to other networks or the Internet. A WAN configuration can include switched and permanent telephone circuits, terrestrial radio systems and satellite systems.

7.1.1 What You Can Do in This Chapter

- The **Internet Connection** screen ([Section 7.2 on page 73](#)) lets you set up your MAX-207HW2R's Internet settings.
- The **WiMAX Configuration** screen ([Section 7.3 on page 75](#)) lets set up the frequencies used by your MAX-207HW2R.
- The **WiMAX FC Table** screen ([Section 7.4 on page 80](#)) lets you view BS information previously scanned by your MAX-207HW2R.

7.1.2 What You Need to Know

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

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is the IEEE 802.16 wireless networking standard, which provides high-bandwidth, wide-range wireless service across wireless Metropolitan Area Networks (MANs). ZyXEL is a member of the WiMAX Forum, the industry group dedicated to promoting and certifying interoperability of wireless broadband products.

In a wireless MAN, a wireless-equipped computer is known either as a mobile station (MS) or a subscriber station (SS). Mobile stations use the IEEE 802.16e standard and are able to maintain connectivity while switching their connection from one base station to another base station (handover) while subscriber stations use other standards that do not have this capability (IEEE 802.16-2004, for

example). The following figure shows an MS-equipped notebook computer **MS1** moving from base station **BS1**'s coverage area and connecting to **BS2**.

Figure 25 WiMax: Mobile Station



WiMAX technology uses radio signals (around 2 to 10 GHz) to connect subscriber stations and mobile stations to local base stations. Numerous subscriber stations and mobile stations connect to the network through a single base station (BS), as in the following figure.

Figure 26 WiMAX: Multiple Mobile Stations



A base station's coverage area can extend over many hundreds of meters, even under poor conditions. A base station provides network access to subscriber stations and mobile stations, and communicates with other base stations.

The radio frequency and bandwidth of the link between the MAX-207HW2R and the base station are controlled by the base station. The MAX-207HW2R follows the base station's configuration.

Authentication

When authenticating a user, the base station uses a third-party RADIUS or Diameter server known as an AAA (Authentication, Authorization and Accounting) server to authenticate the mobile or subscriber stations.

The following figure shows a base station using an **AAA** server to authenticate mobile station **MS**, allowing it to access the Internet.

Figure 27 Using an AAA Server



In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

7.2 Internet Connection

Click **ADVANCED > WAN Configuration** to set up your MAX-207HW2R's Internet settings.

Figure 28 ADVANCED > WAN Configuration > Internet Connection

The following table describes the labels in this screen.

Table 23 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
User	Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters.

Table 23 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access (continued)

LABEL	DESCRIPTION
Password	Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters.
Anonymous Identity	<p>Enter the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption. The anonymous identity is used to route your authentication request to the correct authentication server, and does not reveal your real user name. Your real user name and password are encrypted in the TLS tunnel, and only the anonymous identity can be seen.</p> <p>Leave this field blank if your ISP did not give you an anonymous identity to use.</p>
PKM	This field displays the Privacy Key Management version number. PKM provides security between the MAX-207HW2R and the base station. At the time of writing, the MAX-207HW2R supports PKMv2 only. See the WiMAX security appendix for more information.
Authentication	<p>This field displays the user authentication method. Authentication is the process of confirming the identity of a mobile station (by means of a username and password, for example).</p> <p>Check with your service provider if you are unsure of the correct setting for your account.</p> <p>Choose from the following user authentication methods:</p> <ul style="list-style-type: none"> • TTLS (Tunnelled Transport Layer Security) • TLS (Transport Layer Security) <p>Note: Not all MAX-207HW2Rs support TLS authentication. Check with your service provider for details.</p>
TTLS Inner EAP	<p>This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details.</p> <p>This field is available only when TTLS is selected in the Authentication field.</p> <p>The MAX-207HW2R supports the following inner authentication types:</p> <ul style="list-style-type: none"> • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2)

Table 23 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access (continued)

LABEL	DESCRIPTION
Auth Mode	Select the authentication mode from the drop-down list box. This field is not available in all MAX-207HW2Rs. Check with your service provider for details. The MAX-207HW2R supports the following authentication modes: <ul style="list-style-type: none"> • User Only • Device Only with Cert • Certs and User Authentication
Certificate	This is the security certificate the MAX-207HW2R uses to authenticate the AAA server. Use the TOOLS > Certificate > Trusted CAs screen to import certificates to the MAX-207HW2R.
WAN IP Address Assignment	
Get automatically from ISP (Default)	Select this if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Use Fixed IP Address	A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the IP Address field below.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

7.3 WiMAX Configuration

Click **ADVANCED > WAN Configuration > WiMAX Configuration** to set up the frequencies used by your MAX-207HW2R.

In a WiMAX network, a mobile or subscriber station must use a radio frequency supported by the base station to communicate. When the MAX-207HW2R looks for a connection to a base station, it can search a range of frequencies.

Radio frequency is measured in Hertz (Hz).

Table 24 Radio Frequency Conversion

1 kHz = 1000 Hz
1 MHz = 1000 kHz (1000000 Hz)
1 GHz = 1000 MHz (1000000 kHz)

Figure 29 ADVANCED > WAN Configuration > WiMAX Configuration

The screenshot shows the 'WiMAX Configuration' screen. It is divided into several sections:

- RF Channel List:** A table with 10 rows, each containing 'DL Frequency' and 'Bandwidth' input fields.
- RF Channel Plan:** A section with 9 'Channel Plan' entries (1-9). Each entry includes 'First Frequency', 'Next Step Frequency', 'Last Frequency', and 'Bandwidth' fields.
- Network Access Provider ID:** A section with 6 'Provider' entries (1-6). Each entry includes 'NAP ID', 'Priority', and 'Referenced Channel Plan' fields.
- BS:** A section with radio buttons for 'ALL', 'NEC', 'SAMSUNG', 'MOTO', 'AVARISON', and 'HUAWEI/ZTE'.
- Function Enable:** A section with checkboxes for 'HARQ', 'ARIQ', 'MIMO', 'Idle_Mode', and 'Enable Handover'.

At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 25 ADVANCED > WAN Configuration > WiMAX Configuration

LABEL	DESCRIPTION
RF Channel List	
DL Frequency / Bandwidth	These fields are the downlink frequency settings and bandwidth in kilohertz (kHz). Enter values in these fields to have the MAX-207HW2R scan these frequencies for available channels in ascending numerical order. Contact your service provider for details of supported frequencies.
RF Channel Plan	

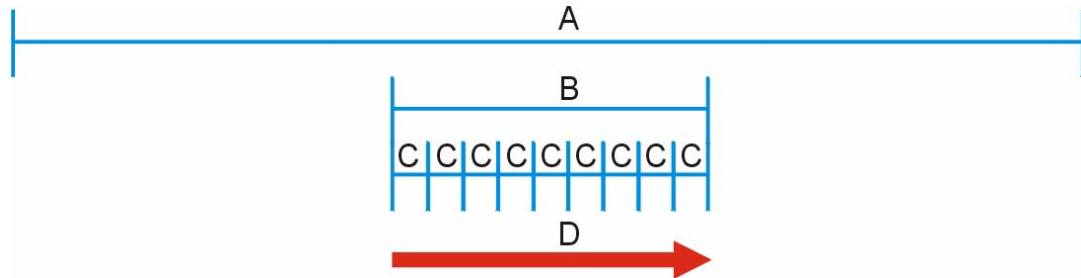
Table 25 ADVANCED > WAN Configuration > WiMAX Configuration (continued)

LABEL	DESCRIPTION
First/Last/Next Step Frequency & Bandwidth	<p>These fields are the downlink frequency settings and bandwidth in kilohertz (kHz).</p> <p>In the First/Last Frequency fields, enter the range of frequency for the MAX-207HW2R to scan for available channels</p> <p>In the Next Step Frequency field, enter the value of the frequency to scan each time that the MAX-207HW2R searches for a connection.</p> <p>Contact your service provider for the bandwidth value and the supported frequencies.</p>
Network Access Provider ID	
NAP ID	Enter the primary network access provider ID for the WAN connection. You can also enter the substitute access provider IDs for the connection backup when the primary one is down.
Priority	Enter the priority of the provider. You may set the priority from 1 to 250.
Reference Channel Plan	Select which RF Channel Plan this provider is referring to.
BS	Select the base station to connect this MAX-207HW2R to.
Function Enable	<p>Select one or multiple check box(es) to enable the function(s). Configure this according to what you were given by your service provider.</p> <ul style="list-style-type: none"> • HARQ: Select this to enable the Hybrid Automatic Repeat-Request feature on the MAX-207HW2R. HARQ works in the physical (PHY) layer and provides radio link error detection and correction. • ARQ: Select this to enable the Automatic Repeat-Request feature on the MAX-207HW2R. ARQ works in the MAC layer and provides error correction by scheduling re-transmission. <p>Both HARQ and ARQ are designed to provide reliable transmission over a wireless connection. When a receiver detects errors, it will notify the sender to retransmit the data within a certain period.</p> <ul style="list-style-type: none"> • MIMO: Select this to enable the Multiple Input Multiple Output (MIMO) feature on the MAX-207HW2R. • Idle_Mode: Select this to have the MAX-207HW2R enter the idle mode after it has no traffic passing through for a pre-defined period. Make sure your base station also supports this before selecting this. • Enable Handover: Select this to maintain connectivity while the MAX-207HW2R switch connection from one base station to another base station.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

7.3.1 Frequency Ranges

The following figure shows the MAX-207HW2R searching a range of frequencies to find a connection to a base station.

Figure 30 Frequency Ranges



In this figure, **A** is the WiMAX frequency range. “WiMAX frequency range” refers to the entire range of frequencies the MAX-207HW2R is capable of using to transmit and receive (see the Product Specifications appendix for details).

In the figure, **B** shows the operator frequency range. This is the range of frequencies within the WiMAX frequency range supported by your operator (service provider).

The operator range is subdivided into bandwidth steps. In the figure, each **C** is a bandwidth step.

The arrow **D** shows the MAX-207HW2R searching for a connection.

Have the MAX-207HW2R search only certain frequencies by configuring the downlink frequencies. Your operator can give you information on the supported frequencies.

The downlink frequencies are points of the frequency range your MAX-207HW2R searches for an available connection. Use the **Site Survey** screen to set these bands. You can set the downlink frequencies anywhere within the WiMAX frequency range. In this example, the downlink frequencies have been set to search all of the operator range for a connection.

7.3.2 Configuring Frequency Settings

You need to set the MAX-207HW2R to scan one or more specific radio frequencies to find an available connection to a WiMAX base station.

Use the **WiMAX Configuration** screen to define the radio frequencies to be searched for available wireless connections.

Note: It may take several minutes for the MAX-207HW2R to find a connection.

- The MAX-207HW2R searches the **DL Frequency** settings in ascending numerical order, from **[1]** to **[10]**.
- If you enter a 0 in a **DL Frequency** field, the MAX-207HW2R immediately moves on to the next **DL Frequency** field.
- When the MAX-207HW2R connects to a base station, the values in this screen are automatically set to the base station's frequency. The next time the MAX-207HW2R searches for a connection, it searches only this frequency. If you want the MAX-207HW2R to search other frequencies, enter them in the **DL Frequency** fields.

The following table describes some examples of **DL Frequency** settings.

Table 26 DL Frequency Example Settings

	EXAMPLE 1	EXAMPLE 2
DL Frequency [1]:	2500000	2500000
DL Frequency [2]:	2550000	2550000
DL Frequency [3]:	0	2600000
DL Frequency [4]:	0	0
	The MAX-207HW2R searches at 2500000 kHz, and then searches at 2550000 kHz if it has not found a connection.	<i>The MAX-207HW2R searches at 2500000 kHz and then at 2550000 kHz if it has not found an available connection. If it still does not find an available connection, it searches at 2600000 kHz.</i>

7.4 WiMAX FC Table

The MAX-207HW2R connects to a WiMAX base station (BS) for Internet access. The WiMAX FC (Frequency Counter) Table screen is a read-only screen that shows a list of the base stations information recently scanned by the MAX-207HW2R.

Figure 31 ADVANCED > WAN Configuration > WiMAX FC Table

BSID	Preamble ID	NAP ID	Frequency(kHz)	Bandwidth(kHz)	RSSI(dBm)	CINR(dB)
00:B6:12:01:13:21	47	00b612	2600000	10000	-63	23
00:B6:12:01:23:22	47	00b612	2620000	10000	-62	18
00:B6:12:01:21:02	77	00b612	2610000	10000	-89	-1
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0
00:00:00:00:00:00	0	000000	0	0	0	0

The following table describes the labels in this screen.

Table 27 ADVANCED > WAN Configuration > WiMAX FC Table

LABEL	DESCRIPTION
Most recently scanned WiMAX BS Table	
Flush Table	Select this check box to clear all the BS information in the WiMAX FC Table.
BSID	This field displays the identification number of the wireless base station to which the MAX-207HW2R is connected. Every base station transmits a unique BSID, which identifies it across the network.
Preamble ID	This field displays the preamble id of the base station. A preamble is an index identifier in the header of the base station's broadcast messages. In the beginning of a mobile station's network entry process, the mobile station searches the preamble and uses it to get further channel characteristics information. It is used to synchronize the upstream and downstream transmission timing with the base station.
NAP ID	This field displays the primary network access provider ID for the WAN connection.
Frequency (KHz)	This field shows the downlink frequency of the base station in kilohertz (kHz).

Table 27 ADVANCED > WAN Configuration > WiMAX FC Table (continued)

LABEL	DESCRIPTION
Bandwidth (KHz)	This field shows the bandwidth of the base station in kilohertz (kHz).
RSSI (dBm)	<p>This field shows the Received Signal Strength Indication. This value is a measurement of overall radio signal strength. A higher RSSI level indicates a stronger signal, and a lower RSSI level indicates a weaker signal.</p> <p>A strong signal does not necessarily indicate a good signal: a strong signal may have a low signal-to-noise ratio (SNR).</p>
CINR (dB)	This field shows the average Carrier to Interference plus Noise Ratio of the current connection. This value is an indication of overall radio signal quality. A higher value indicates a higher signal quality, and a lower value indicates a lower signal quality.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

The Port Configuration Screens

8.1 Overview

Use these screens to enable NAT and configure port forwarding for the MAX-207HW2R.

Network Address Translation (NAT) maps a host's IP address within one network to a different IP address in another network. For example, you can use a NAT router to map one IP address from your ISP to multiple private IP addresses for the devices in your home network.

8.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 8.2 on page 84](#)) lets you enable or disable NAT and to allocate memory for NAT and firewall rules.
- The **Port Forwarding** screen ([Section 8.3 on page 85](#)) lets you look at the current port-forwarding rules in the MAX-207HW2R, and to enable, disable, activate, and deactivate each one.

8.2 General

Click **ADVANCED > NAT Configuration > General** to enable or disable NAT and to allocate memory for NAT and firewall rules.

Figure 32 ADVANCED > NAT Configuration > General

The screenshot shows a configuration window with two tabs: 'General' and 'Port Forwarding'. The 'General' tab is active. It contains a checked checkbox for 'Enable Network Address Translation' and a text input field for 'Max NAT/Firewall Session Per User' with the value '2048'. At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 28 ADVANCED > NAT Configuration > General

LABEL	DESCRIPTION
Enable Network Address Translation	Select this if you want to enable the Network Address Translation.
Max NAT/Firewall Session Per User	<p>When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the MAX-207HW2R.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.</p>
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

8.3 Port Forwarding

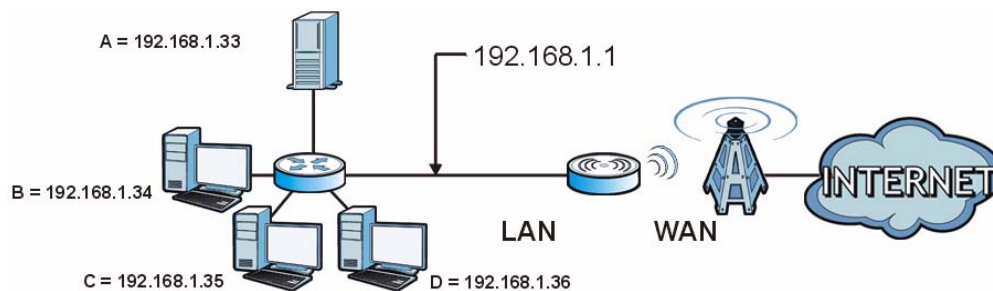
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **ADVANCED > NAT Configuration > Port Forwarding** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

For example, let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 33 Multiple Servers Behind NAT Example

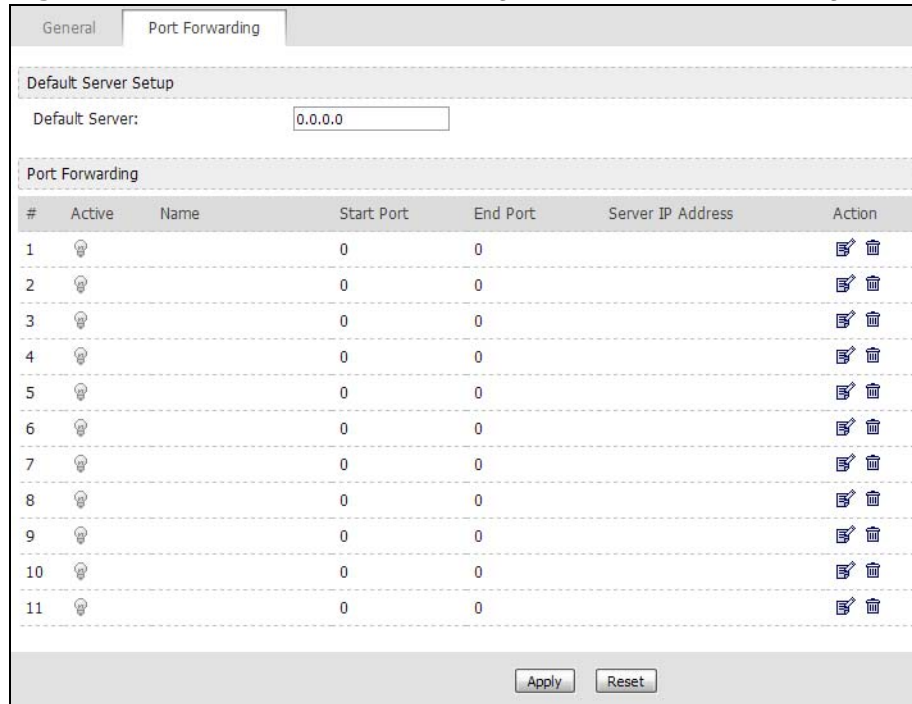


8.3.1 Port Forwarding Options

Click **ADVANCED > NAT Configuration > Port Forwarding** to look at the current port-forwarding rules in the MAX-207HW2R, and to enable, disable,



activate, and deactivate each one. You can also set up a default server to handle ports not covered by rules.

Figure 34 ADVANCED > NAT Configuration > Port Forwarding



The following table describes the icons in this screen.

Table 29 ADVANCED > NAT Configuration > Port Forwarding

ICON	DESCRIPTION
	Edit Click to edit this item.
	Delete Click to delete this item.

The following table describes the labels in this screen.

Table 30 ADVANCED > NAT Configuration > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	Enter the IP address of the server to which the MAX-207HW2R should forward packets for ports that are not specified in the Port Forwarding section below or in the TOOLS > Remote MGMT screens. Enter 0.0.0.0 if you want the MAX-207HW2R to discard these packets instead.
Port Forwarding	
#	The number of the item in this list.
Active	Select this to enable this rule. Clear this to disable this rule.

Table 30 ADVANCED > NAT Configuration > Port Forwarding (continued)

LABEL	DESCRIPTION
Name	This field displays the name of the rule. It does not have to be unique.
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the Start Port , only one port number is forwarded.
Server IP Address	This field displays the IP address of the server to which packet for the selected port(s) are forwarded.
Action	Click the Edit icon to set up a port forwarding rule or alter the configuration of an existing port forwarding rule. Click the Delete icon to remove an existing port forwarding rule.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

8.3.2 Port Forwarding Rule Setup

Click a port forwarding rule's **Edit** icon in the **ADVANCED > NAT Configuration > Port Forwarding** screen to activate, deactivate, or edit it.

Figure 35 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

The following table describes the labels in this screen.

Table 31 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

LABEL	DESCRIPTION
Rule Setup	
Active	Select this to enable this rule. Clear this to disable this rule.
Service Name	Enter a name to identify this rule. You can use 1 - 31 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.

Table 31 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

LABEL	DESCRIPTION
Start Port End Port	Enter the port number or range of port numbers you want to forward to the specified server. To forward one port number, enter the port number in the Start Port and End Port fields. To forward a range of ports, <ul style="list-style-type: none">• enter the port number at the beginning of the range in the Start Port field• enter the port number at the end of the range in the End Port field.
Server IP Address	Enter the IP address of the server to which to forward packets for the selected port number(s). This server is usually on the LAN.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

The System Configuration Screens

9.1 Overview

Click **ADVANCED > System Configuration** to set up general system settings, change the system mode, change the password, configure the DDNS server settings, and set the current date and time.

9.1.1 What You Can Do in This Chapter

- The **Dynamic DNS** screen ([Section 9.2 on page 90](#)) lets you set up the MAX-207HW2R as a dynamic DNS client.
- The **Firmware** screen ([Section 9.3 on page 92](#)) lets you upload new firmware to the MAX-207HW2R.
- The **Configuration** screen ([Section 9.4 on page 93](#)) lets you back up or restore the configuration of the MAX-207HW2R.
- The **Restart** screen ([Section 9.5 on page 95](#)) lets you restart your MAX-207HW2R from within the web configurator.

9.1.2 What You Need to Know

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

System Name

The **System Name** is often used for identification purposes. Because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 2000: Click **Start > Settings > Control Panel** and then double-click the **System** icon. Select the **Network Identification** tab and then click the **Properties** button. Note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows XP: Click **Start > My Computer > View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the MAX-207HW2R **System Name**.

Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the MAX-207HW2R via DHCP.

DNS Server Address Assignment

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

The MAX-207HW2R can get the DNS server addresses in the following ways:

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **SYSTEM General** screen.
- 2 If the ISP did not give you DNS server information, leave the **DNS Server** fields in the **SYSTEM General** screen set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

9.2 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dns.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

Click **ADVANCED > System Configuration > Dynamic DNS** to set up the MAX-207HW2R as a dynamic DNS client.

Figure 36 ADVANCED > System Configuration > Dynamic DNS

The following table describes the labels in this screen.

Table 32 ADVANCED > System Configuration > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Enable Dynamic DNS	Select this to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Enter the host name. You can specify up to two host names, separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select this to enable the DynDNS Wildcard feature.
Enable offline option (Only applies to custom DNS)	This field is available when CustomDNS is selected in the DDNS Type field. Select this if your Dynamic DNS service provider redirects traffic to a URL that you can specify while you are off line. Check with your Dynamic DNS service provider.
IP Address Update Policy	
Use WAN IP Address	Select this if you want the MAX-207HW2R to update the domain name with the WAN port's IP address.

Table 32 ADVANCED > System Configuration > Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP address	Select this if you want the DDNS server to update the IP address of the host name(s) automatically. Select this option when there are one or more NAT routers between the MAX-207HW2R and the DDNS server. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the MAX-207HW2R and the DDNS server.
Use specified IP address	Select this if you want to use the specified IP address with the host name(s). Then, specify the IP address. Use this option if you have a static IP address.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

9.3 Firmware

Click **ADVANCED > System Configuration > Firmware** to upload new firmware to the MAX-207HW2R. Firmware files usually use the system model name with a "*.bin" extension, such as "MAX-207HW2R.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Contact your service provider for information on available firmware upgrades.

Note: Only use firmware for your MAX-207HW2R's specific model.

Figure 37 ADVANCED > System Configuration > Firmware

The following table describes the labels in this screen.

Table 33 ADVANCED > System Configuration > Firmware

LABEL	DESCRIPTION
File Path	Enter the location of the *.bin file you want to upload, or click Browse... to find it. You must decompress compressed (.zip) files before you can upload them.

Table 33 ADVANCED > System Configuration > Firmware (continued)

LABEL	DESCRIPTION
Browse...	Click this to find the *.bin file you want to upload.
Upload	Click this to begin uploading the selected file. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress!

9.3.1 The Firmware Upload Process

When the MAX-207HW2R uploads new firmware, the process usually takes about two minutes. The device also automatically restarts in this time. This causes a temporary network disconnect.

Note: Do not turn off the device while firmware upload is in progress!

After two minutes, log in again, and check your new firmware version in the **Status** screen. You might have to open a new browser window to log in.

If the upload is not successful, you will be notified by error message.

Click **Return** to go back to the **Firmware** screen.

9.4 Configuration

Click **ADVANCED > System Configuration > Configuration** to back up or restore the configuration of the MAX-207HW2R. You can also use this screen to reset the MAX-207HW2R to the factory default settings.

Figure 38 ADVANCED > System Configuration > Configuration

Dynamic DNS Firmware Configuration Restart

Backup Configuration

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

Restore Configuration

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

File Path:

Back to Factory Defaults

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

- Password will be default value
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

The following table describes the labels in this screen.

Table 34 ADVANCED > System Configuration > Configuration

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click this to save the MAX-207HW2R's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.
Restore Configuration	
File Path ()	Enter the location of the file you want to upload, or click Browse... to find it.
Browse	Click this to find the file you want to upload.
Upload	Click this to restore the selected configuration file. Note: Do not turn off the device while configuration file upload is in progress.
Back to Factory Defaults	
Reset	Click this to clear all user-entered configuration information and return the MAX-207HW2R to its factory defaults. There is no warning screen.

9.4.1 The Restore Configuration Process

When the MAX-207HW2R restores a configuration file, the device automatically restarts. This causes a temporary network disconnect.

Note: Do not turn off the device while configuration file upload is in progress.

If the MAX-207HW2R's IP address is different in the configuration file you selected, you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See the Quick Start Guide or the appendices for details on how to set up your computer's IP address.

You might have to open a new browser to log in again.

If the upload was not successful, you are notified by **Configuration Upload Error** message:

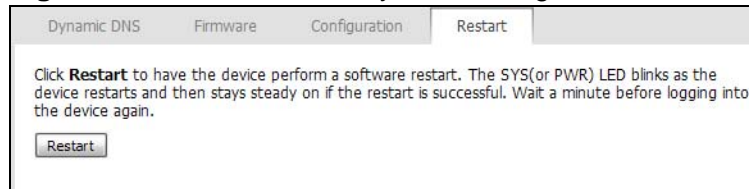
Click **Return** to go back to the **Configuration** screen.

9.5 Restart

Click **ADVANCED > System Configuration > Restart** to reboot the MAX-207HW2R without turning the power off.

Note: Restarting the MAX-207HW2R does not affect its configuration.

Figure 39 ADVANCED > System Configuration > Restart



The following table describes the labels in this screen.

Table 35 ADVANCED > System Configuration > Firmware

LABEL	DESCRIPTION
Restart	<p>Click this button to have the device perform a software restart. The Power LED blinks as it restarts and the shines steadily if the restart is successful.</p> <p>Note: Wait one minute before logging back into the MAX-207HW2R after a restart.</p>

9.5.1 The Restart Process

When you click **Restart**, the the process usually takes about two minutes. Once the restart is complete you can log in again.

The Service Configuration Screens

10.1 Overview

The **VOICE > Service Configuration** screens allow you to set up your voice accounts and configure your QoS settings.

VoIP (Voice over IP) is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service. A company could alternatively set up an IP-PBX and provide its own VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

10.1.1 What You Can Do in This Chapter

- The **SIP Setting** screen ([Section 10.2 on page 99](#)) lets you setup and maintain your SIP account(s) in the MAX-207HW2R.
- The **Advanced SIP Settings** screen ([Section 10.2.1 on page 100](#)) lets you set up and maintain advanced settings for each SIP account

10.1.2 What You Need to Know

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

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can

use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider (the company that lets you make phone calls over the Internet) is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

Use NAT

If you know the NAT router's public IP address and SIP port number, you can use the Use NAT feature to manually configure the MAX-207HW2R to use a them in the SIP messages. This eliminates the need for STUN or a SIP ALG. You must also configure the NAT router to forward traffic with this port number to the MAX-207HW2R.

10.1.3 Before you Begin

- Ensure that you have all of your voice account information on hand. If not, contact your voice account service provider to find out which settings in this chapter you should configure in order to use your telephone with the MAX-207HW2R.
- Connect your MAX-207HW2R to the Internet, as described in the Quick Start Guide. If you have not already done so, then you will not be able to test your VoIP settings.

10.2 SIP Settings

Click **VOICE > Service Configuration > SIP Setting** to setup and maintain your SIP account(s) in the MAX-207HW2R. Your VoIP or Internet service provider should provide you with your account information. You can also enable and disable each SIP account.

Figure 40 VOICE > Service Configuration > SIP Setting

The following table describes the labels in this screen.

Table 36 VOICE > Service Configuration > SIP Setting

LABEL	DESCRIPTION
SIP Account	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
SIP Settings	
Active SIP Account	Select this if you want the MAX-207HW2R to use this account. Clear it if you do not want the MAX-207HW2R to use this account.
Phone Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.

Table 36 VOICE > Service Configuration > SIP Setting (continued)

LABEL	DESCRIPTION
SIP Local Port	Enter the MAX-207HW2R's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
Show Advanced Setup	Click this to display the advanced settings for this SIP account in this screen for editing.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

10.2.1 Advanced SIP Settings

This section describes the features of the Advanced SIP settings screen.

10.2.1.1 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The MAX-207HW2R supports the following codecs.

- **G.711** is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals (sampling) and converts them into digital bits (quantization). Quantization “reads” the analog signal and then “writes” it to the nearest digital value. For this reason, a digital sample is usually slightly different from its analog original (this difference is known as “quantization noise”). G.711 provides excellent sound quality but requires 64kbps of bandwidth.
- **G.723** is an Adaptive Differential Pulse Code Modulation (ADPCM) waveform codec. Differential (or Delta) PCM is similar to PCM, but encodes the audio signal based on the difference between one sample and a prediction based on previous samples, rather than encoding the sample’s actual quantized value. Many thousands of samples are taken each second, and the differences between consecutive samples are usually quite small, so this saves space and reduces the bandwidth necessary.

However, DPCM produces a high quality signal (high signal-to-noise ratio or SNR) for high difference signals (where the actual signal is very different from what was predicted) but a poor quality signal (low SNR) for low difference signals (where the actual signal is very similar to what was predicted). This is because the level of quantization noise is the same at all signal levels. Adaptive DPCM solves this problem by adapting the difference signal’s level of quantization according to the audio signal’s strength. A low difference signal is given a higher quantization level, increasing its signal-to-noise ratio. This provides a similar sound quality at all signal levels. G.723 provides high quality sound and requires 20 or 40 kbps.

- **G.729** is an Analysis-by-Synthesis (AbS) hybrid waveform codec. It uses a filter based on information about how the human vocal tract produces sounds. The codec analyzes the incoming voice signal and attempts to synthesize it using its list of voice elements. It tests the synthesized signal against the original and, if it is acceptable, transmits details of the voice elements it used to make the synthesis. Because the codec at the receiving end has the same list, it can exactly recreate the synthesized audio signal. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

10.2.1.2 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have one or more voice messages. Your VoIP service provider must have a messaging system that sends message–waiting–status SIP packets as defined in RFC 3842.

10.2.1.3 Advanced SIP Settings Options

Click **Show Advanced Setup** in **VOICE > Service Configuration > SIP Settings** to set up and maintain advanced settings for each SIP account.

Figure 41 VOICE > Service Configuration > SIP Settings > Show Advanced Setup

The screenshot shows the 'Show Advanced Setup' screen for SIP settings. It is organized into several sections:

- SIP Server Settings:** Includes fields for URL Type (dropdown), Register Expiration Duration (3600), Register Fail Re-register Timer (180), Session Expires(SE) (180), and Min-SE (30).
- RTP Port Range:** Includes Start Port (30000) and End Port (35000).
- Voice Compression:** Includes Primary, Secondary, and Third Compression Type (dropdowns) and DTMF Mode (RFC 2833).
- MWI (Message Waiting Indication):** Includes an 'Enable' checkbox and Expiration Time (1800).
- Fax Option:** Includes radio buttons for G.711 Fax Passthrough and T.38 Fax Relay.
- Call Waiting:** Includes an 'Enable' checkbox and Call Waiting Reject Time (20).
- Call Transfer:** Includes an 'Enable' checkbox.
- Call Forward:** Includes Call Forward Table (Table 1).
- Call Conference:** Includes an 'Enable' checkbox.
- Early Media:** Includes an 'Enable' checkbox and Early Media Tone (Default).
- Music on Hold:** Includes an 'Enable' checkbox and Music-on-Hold Tone (Default).

At the bottom of the screen, there is a 'Hide Advanced Setup' button and 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 37 VOICE > Service Configuration > SIP Settings > Show Advanced Setup

LABEL	DESCRIPTION
SIP Server Settings	
URL Type	Select whether or not to include the SIP service domain name when the MAX-207HW2R sends the SIP number. <ul style="list-style-type: none"> • SIP - include the SIP service domain name • TEL - do not include the SIP service domain name

Table 37 VOICE > Service Configuration > SIP Settings > Show Advanced Setup

LABEL	DESCRIPTION
Register Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The MAX-207HW2R automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send Timer	Enter the number of seconds the MAX-207HW2R waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires (SE)	Enter the number of seconds the conversation can last before the call is automatically disconnected. Usually, when one-half of this time has passed, the MAX-207HW2R or the other party updates this timer to prevent this from happening.
Min-SE	Enter the minimum number of seconds the MAX-207HW2R accepts for a session expiration time when it receives a request to start a SIP session. If the request has a shorter time, the MAX-207HW2R rejects it.
RTP Port Range	
Start Port End Port	<p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the Start Port and End Port fields.</p> <p>To enter a range of ports:</p> <ul style="list-style-type: none"> Type the port number at the beginning of the range in the Start Port field Type the port number at the end of the range in the End Port field.
Voice Compression	
Primary, Secondary, and Third Compression	<p>Select the type of voice coder/decoder (codec) that you want the MAX-207HW2R to use.</p> <p>G.711 provides high voice quality but requires more bandwidth (64 kbps).</p> <ul style="list-style-type: none"> G.729 requires only 8 kbps. G.711A is typically used in Europe. G.711u is typically used in North America and Japan. G.723 provides good voice quality, and requires 20 or 40 kbps. <p>The MAX-207HW2R must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.</p> <p>For more on voice compression, see Voice Coding on page 100</p> <p>DTMF Mode controls how the MAX-207HW2R handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.</p> <ul style="list-style-type: none"> RFC 2833 - send the DTMF tones in RTP packets. PCM - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. SIP INFO - send the DTMF tones in SIP messages.

Table 37 VOICE > Service Configuration > SIP Settings > Show Advanced Setup

LABEL	DESCRIPTION
MWI (Message Waiting Indication)	
Enable	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the MAX-207HW2R subscribes to the service. Before this time passes, the MAX-207HW2R automatically subscribes again.
Fax Option	
G.711 Fax Passthrough	Select this if the MAX-207HW2R should use G.711 to send fax messages. The peer devices must also use G.711.
T.38 Fax Relay	Select this if the MAX-207HW2R should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Call Waiting	
Enable	Check this if you want to place a call on hold while you answer another incoming call on the same telephone number.
Call Waiting Reject Time	Enter the number of seconds the MAX-207HW2R should wait for you to answer an incoming call before it considers the call is unanswered.
Call Transfer	
Enable	Check this if you want to transfer an incoming call that you have answered to another phone.
Call Forward	
Call Forward Table	Select which call forwarding table you want the MAX-207HW2R to use for incoming calls. You set up these tables in VOICE > Phone Book > Incoming Call Policy .
Call Conference	
Enable	Check this box if you want to make conference calls.
Early Media	
Enable	Check this box if you want people to hear a customized recording when they call you.
Early Media Tone	Select the tone you want people to hear when they call you. See Custom Tones (IVR) on page 105 for information on how to record these tones.
Music on Hold	
Enable	Check this box if you want people to hear a customized recording when you put them on hold.
Music-on-Hold Tone	Select the tone you want people to hear when you put them on hold. See Custom Tones (IVR) on page 105 for information on how to record these tones.
Hide Advanced Setup	Click this to not display these advanced settings in this screen.

10.2.1.4 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the MAX-207HW2R. The MAX-207HW2R allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 38 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	128 seconds for all custom tones combined
Maximum Time per Individual Tone	20 seconds
Total Number of Tones Recordable	8 You can record up to eight different custom tones but the total time must be 128 seconds or less.

Use the following steps if you would like to create new tones or change your tones:

- 1 Pick up the phone and press ******** on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1101~1108 on your phone followed by the **#** key.
- 3 Play your desired music or voice recording into the receiver's mouthpiece. Press the **#** key.
- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Do the following to listen to a custom tone:

- 1 Pick up the phone and press ******** on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1201~1208 followed by the **#** key to listen to the tone.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Do the following to delete a custom tone:

- 1 Pick up the phone and press ******** on your phone's keypad and wait for the message that says you are in the configuration menu.

- 2 Press a number from 1301~1308 followed by the # key to delete the tone of your choice. Press 14 followed by the # key if you wish to clear all your custom tones.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

10.3 Technical Reference

The following section contains additional technical information about the MAX-207HW2R features described in this chapter.

10.3.1 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 39 SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK
4. ACK		
	5. Dialogue (voice traffic)	
6. BYE		
		7. OK

- 1 A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
- 2 B sends a response indicating that the telephone is ringing.
- 3 B sends an OK response after the call is answered.
- 4 A then sends an ACK message to acknowledge that B has answered the call.
- 5 Now A and B exchange voice media (talk).
- 6 After talking, A hangs up and sends a BYE request.
- 7 B replies with an OK response confirming receipt of the BYE request and the call is terminated.

10.3.2 SIP Client Server

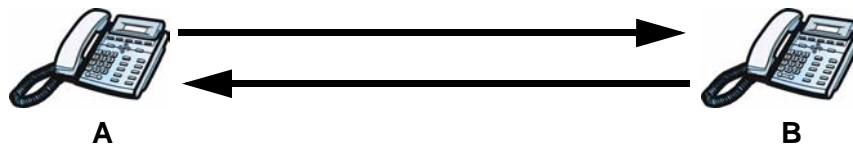
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

10.3.3 SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent to receive the call.

Figure 42 SIP User Agent



10.3.4 SIP Proxy Server

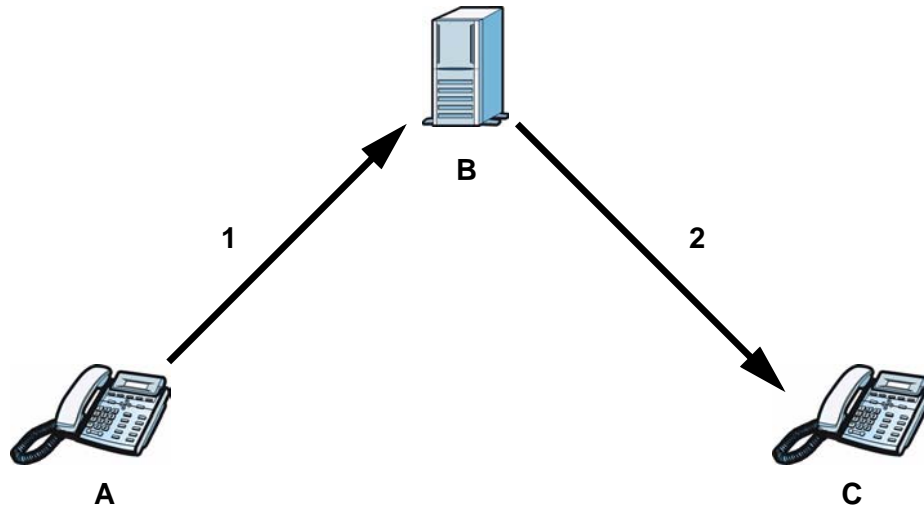
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 The client device (A in the figure) sends a call invitation to the SIP proxy server (B).

- 2 The SIP proxy server forwards the call invitation to C.

Figure 43 SIP Proxy Server



10.3.5 SIP Redirect Server

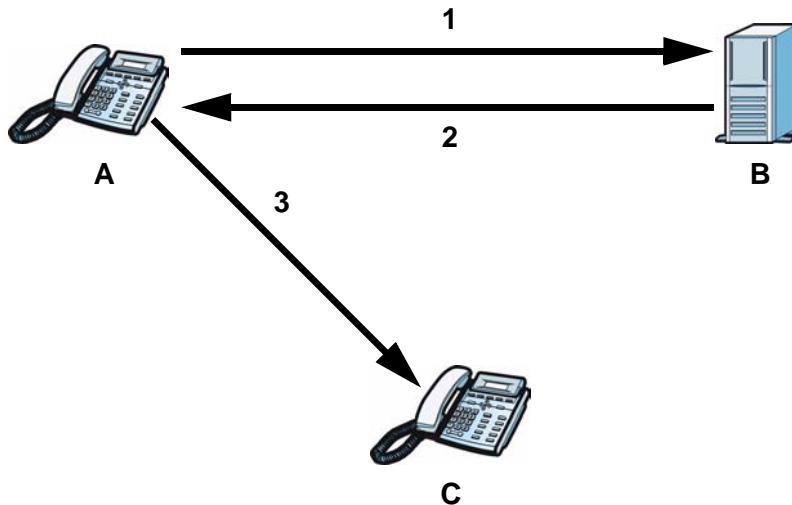
A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 Client device A sends a call invitation for C to the SIP redirect server (B).
- 2 The SIP redirect server sends the invitation back to A with C's IP address (or domain name).

- 3 Client device A then sends the call invitation to client device C.

Figure 44 SIP Redirect Server



10.3.6 NAT and SIP

The MAX-207HW2R must register its public IP address with a SIP register server. If there is a NAT router between the MAX-207HW2R and the SIP register server, the MAX-207HW2R probably has a private IP address. The MAX-207HW2R lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the MAX-207HW2R's IP address from inside the SIP message and maps it to your SIP identity. If the MAX-207HW2R has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity. See [Chapter 8 The Port Configuration Screens](#) for more information.

Use a SIP ALG (Application Layer Gateway), Use NAT, STUN, or outbound proxy to allow the MAX-207HW2R to list its public IP address in the SIP messages.

10.3.7 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

10.3.8 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

Figure 45 DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)
-----------------	-------------------

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

The Phone Screens

11.1 Overview

Use the **VOICE > Phone** screens to configure the volume, echo cancellation, VAD settings and custom tones for the phone port on the MAX-207HW2R. You can also select which SIP account to use for making outgoing calls.

11.1.1 What You Can Do in This Chapter

- The **Analog Phone** screen ([Section 11.2 on page 112](#)) lets you control which SIP accounts each phone uses.
- The **Common** screen ([Section 11.3 on page 115](#)) lets you activate and deactivate immediate dialing.
- The **Region** screen ([Section 11.4 on page 116](#)) lets you maintain settings that often depend on the region of the world in which the MAX-207HW2R is located.

11.1.2 What You Need to Know

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

Voice Activity Detection/Silence Suppression/Comfort Noise

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the MAX-207HW2R reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

When using VAD, the MAX-207HW2R generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

Supplementary Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The MAX-207HW2R supports the following services:

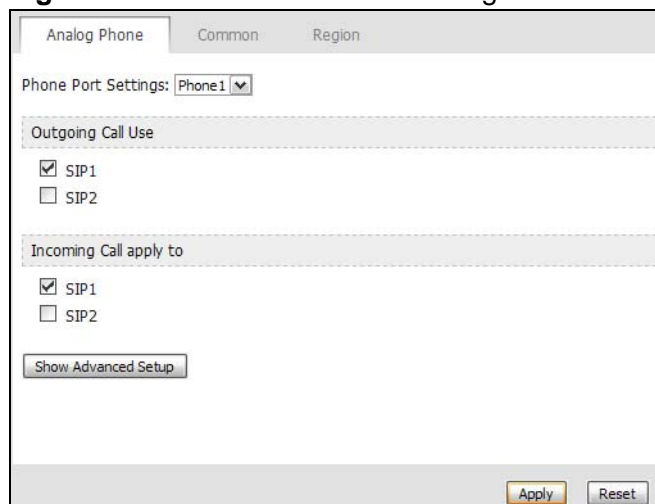
- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Caller ID
- CLIP (Calling Line Identification Presentation)
- CLIR (Calling Line Identification Restriction)

Note: To take full advantage of the supplementary phone services available through the MAX-207HW2R's phone port, you may need to subscribe to the services from your VoIP service provider.

11.2 Analog Phone

Click **VOICE > Phone > Analog Phone** to control which SIP accounts each phone uses.

Figure 46 VOICE > Phone > Analog Phone



The screenshot shows the configuration page for an Analog Phone. At the top, there are three tabs: "Analog Phone" (selected), "Common", and "Region". Below the tabs, the "Phone Port Settings" are set to "Phone1". The page is divided into two main sections: "Outgoing Call Use" and "Incoming Call apply to". In the "Outgoing Call Use" section, the "SIP1" checkbox is checked, and the "SIP2" checkbox is unchecked. In the "Incoming Call apply to" section, the "SIP1" checkbox is checked, and the "SIP2" checkbox is unchecked. At the bottom of the page, there is a "Show Advanced Setup" button and "Apply" and "Reset" buttons.

The following table describes the labels in this screen.

Table 40 VOICE > Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Settings	Select the number of a phone port for the configuration in this screen.
Outgoing Call Use	
SIP1	Select this if you want this phone port to use the SIP1 account when it makes calls. If you select both SIP accounts, the MAX-207HW2R tries to use SIP2 first.
SIP2	Select this if you want this phone port to use the SIP2 account when it makes calls. If you select both SIP accounts, the MAX-207HW2R tries to use SIP2 first.
Incoming Call apply to	
SIP1	Select this if you want to receive phone calls for the SIP1 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
SIP2	Select this if you want to receive phone calls for the SIP2 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
Show Advanced Setup	Click this to edit the advanced settings for this phone port. The advanced settings appear.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

11.2.1 Advanced Analog Phone Setup

Click the **Show Advanced Setup** button in **VOICE > Phone > Analog Phone** to edit advanced settings for the selected phone port.

Figure 47 VOICE > Phone > Analog Phone > Show Advanced Setup

The screenshot shows the 'Show Advanced Setup' screen for an analog phone. It contains the following settings:

- Voice Volume Control:**
 - Speaking Volume: 0 dB
 - Listening Volume: 0 dB
- Echo Cancellation:**
 - G.168 Active
- Dialing Setting:**
 - First Digit Timeout Interval: 8 sec
 - Dialing Digit Timeout Interval: 3 sec
- Voice Activity Detection (VAD):**
 - VAD Support

At the bottom of the screen, there is a 'Hide Advanced Setup' button and 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 41 VOICE > Phone > Analog Phone > Show Advanced Setup

LABEL	DESCRIPTION
Voice Volume Control	
Speaking Volume	Enter the loudness that the MAX-207HW2R uses for speech that it sends to the peer device. -1 is the quietest, and 1 is the loudest.
Listening Volume	Enter the loudness that the MAX-207HW2R uses for speech that it receives from the peer device. -1 is the quietest, and 1 is the loudest.
Echo Cancellation	
G.168 Active	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Dialing Setting	
First Digit Timeout Interval	Set the number of seconds for the MAX-207HW2R to wait for you to start dialing a number after you pick up the telephone receiver. If you do not dial any number within that time period, the dial tone becomes a busy signal. Put back the receiver and pick it up again if you want to make a new call.
Dialing Digit Timeout Interval	Set the interval (in seconds) for the MAX-207HW2R to wait for each subsequent number when dialing. If the interval passes and no new subsequent number is dialed, the MAX-207HW2R attempts to dial with the numbers that were entered.
Voice Activity Detection (VAD)	
VAD Support	Select this if the MAX-207HW2R should stop transmitting when you are not speaking. This reduces the bandwidth the MAX-207HW2R uses.
Hide Advanced Setup	Click this to not display these advanced settings in this screen.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

11.3 Common

Click **VOICE > Phone > Common** to activate and deactivate immediate dialing.

Figure 48 VOICE > Phone > Common

The following table describes the labels in this screen.

Table 42 VOICE > Phone > Common

LABEL	DESCRIPTION
Immediate Dial	
Active Immediate Dial	Select this if you want to use the pound key (#) to tell the MAX-207HW2R to make the phone call immediately, instead of waiting the number of seconds you selected in the Dialing Interval Select in VOICE > Phone > Analog Phone . If you select this, dial the phone number, and then press the pound key if you do not want to wait. The MAX-207HW2R makes the call immediately.
Flash Timer	
Enable Manual Setting	Select this check box to enable the manual setting of the flash key interval timer. You can activate supplementary services of your phone with the flash key (see Section 11.5.1 on page 117 for more information). The configuration for flash key interval timer depends on your country code. It is usually pre-configured on your phone device by its manufacturer. You can set or change it on the MAX-207HW2R if necessary.
Min./Max. Interval	Enter the minimum and maximum timer interval for your flash key. Contact your phone service provider for the setting values used in your country.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

11.4 Region

Click **VOICE > Phone > Region** to maintain settings that often depend on the region of the world in which the MAX-207HW2R is located.

Figure 49 VOICE > Phone > Region

The following table describes the labels in this screen.

Table 43 VOICE > Phone > Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the MAX-207HW2R is located. Do not select Default .
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. <ul style="list-style-type: none"> • Europe Type - use supplementary phone services in European mode • USA Type - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

11.5 Technical Reference

The following section contains additional technical information about the MAX-207HW2R features described in this chapter.

11.5.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. The MAX-207HW2R may interpret manual tapping as hanging up if the duration is too long

You can invoke all the supplementary services by using the flash key.

11.5.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 44 European Type Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold allows you to put a call (A) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.
Press the flash key and then press "0".
- Disconnect the first call and answer the second call.
Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.
Press the flash key and then "2".

European Call Transfer allows you to transfer an incoming call (that you have answered) to another phone. To do so:

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "**98#" followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference allows you to make three-way conference calls. To do so:

- 1 When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call.
- 3 When the second call is answered, press the flash key and press "3" to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

11.5.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 45 USA Type Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

USA Call Hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer allows you to transfer an incoming call (that you have answered) to another phone. To do so:

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "***98#**" followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference allows you to make three-way conference calls. To do so:

- 1** When you are making a call, press the flash key to put the call on hold and get a dial tone.
- 2** Dial a phone number to make a second call.
- 3** When the second call is answered, press the flash key to create a three-way conversation.
- 4** If you want to separate the three-way conference into two individual calls (one call is online, the other is on hold), press the flash key. The first call is online and the second call is on hold. Pressing the flash key again will recreate the three-way conversation. The next time you press the flash key, the second call is online and the first call is on hold.
- 5** Hang up the phone to drop the connection.

The Phone Book Screens

12.1 Overview

The **VOICE > Phone Book** screens allow you to configure the MAX-207HW2R's phone book for making VoIP calls.

12.1.1 What You Can Do in This Chapter

- The **Call Forward Policy** screen ([Section 12.2 on page 122](#)) lets you maintain rules for handling incoming calls. You can block, redirect, or accept them.
- The **Speed Dial** screen ([Section 12.3 on page 124](#)) lets you add, edit, or remove speed-dial entries.

12.1.2 What You Need to Know

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

Speed Dial and Peer-to-Peer Calling

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. It is also required if you want to make peer-to-peer calls.

In peer-to-peer calls, you call another VoIP device directly without going through a SIP server. In the MAX-207HW2R, you must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The MAX-207HW2R sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

You do not need to configure a SIP account in order to make a peer-to-peer VoIP call.

12.2 Call Forward Policy

Click **VOICE > Phone Book > Call Forward Policy** to maintain rules for handling incoming calls. You can block, redirect, or accept them.

Figure 50 VOICE > Phone Book > Call Forward Policy

The following table describes the labels in this screen.

Table 46 VOICE > Phone Book > Call Forward Policy

LABEL	DESCRIPTION
Table Index	Select the call-forwarding table you want to see in this screen. If you change this field, the screen automatically refreshes.
Call Forward Active	Select this check box to enable call forward. You can configure the rules in Advanced Setup - Incoming Call Policy .
Forward to Number Setup	
Unconditional Forward to Number	Select this if you want the MAX-207HW2R to forward all incoming calls to the specified phone number, regardless of other rules in the Forward to Number section. Specify the phone number in the field on the right.
Busy Forward to Number	Select this if you want the MAX-207HW2R to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer Forward to Number	Select this if you want the MAX-207HW2R to forward incoming calls to the specified phone number if the call is unanswered. (See No Answer Waiting Time .) Specify the phone number in the field on the right.

Table 46 VOICE > Phone Book > Call Forward Policy

LABEL	DESCRIPTION
No Answer Waiting Time	This field is used by the No Answer Forward to Number feature and No Answer conditions below. Enter the number of seconds the MAX-207HW2R should wait for you to answer an incoming call before it considers the call is unanswered.
Advanced Setup - Incoming Call Policy	
#	The number of the item in this list.
Activate	Select this to enable this rule. Clear this to disable this rule.
Incoming Call Number	Enter the phone number to which this rule applies.
Forward to Number	Enter the phone number to which you want to forward incoming calls from the Incoming Call Number . You may leave this field blank, depending on the Condition .
Condition	Select the situations in which you want to forward incoming calls from the Incoming Call Number , or select an alternative action. <ul style="list-style-type: none"> • Unconditional - The MAX-207HW2R immediately forwards any calls from the Incoming Call Number to the Forward to Number. • Busy - The MAX-207HW2R forwards any calls from the Incoming Call Number to the Forward to Number when your SIP account already has a call connected. • No Answer - The MAX-207HW2R forwards any calls from the Incoming Call Number to the Forward to Number when the call is unanswered. (See No Answer Waiting Time.) • Block - The MAX-207HW2R rejects calls from the Incoming Call Number. • Accept - The MAX-207HW2R allows calls from the Incoming Call Number. You might create a rule with this condition if you do not want incoming calls from someone to be forwarded by rules in the Forward to Number section.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

Note: The MAX-207HW2R checks the Advanced rules first before checking the Forward to Number rules. All rules are checked in order from top to bottom.

12.3 Speed Dial

Click **VOICE > Phone Book > Speed Dial** to add, edit, or remove speed-dial entries.

You must create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that use letters. You can also create speed-dial entries for frequently-used SIP phone numbers.

Figure 51 VOICE > Phone Book > Speed Dial

Call Forward Policy		Speed Dial			
Speed Dial Number	Active	Original Phone Number	Name (or Memo)	Destination	Action
#01				(Use Proxy)	
#02				(Use Proxy)	
#03				(Use Proxy)	
#04				(Use Proxy)	
#05				(Use Proxy)	
#06				(Use Proxy)	
#07				(Use Proxy)	
#08				(Use Proxy)	
#09				(Use Proxy)	
#10				(Use Proxy)	

The following table describes the icons in this screen.

Table 47 VOICE > Phone Book > Speed Dial

ICON	DESCRIPTION
	Edit Click to edit this item.
	Delete Click to delete this item.

The following table describes the labels in this screen.

Table 48 VOICE > Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial Number	This is a list of speed dial numbers.
Active	This field indicates whether the rule is active or not.
Original Phone Number	This is the original phone number you want the MAX-207HW2R to call when you dial the speed-dial number.
Name (or Memo)	This is the name of the party associated with this speed-dial number.

Table 48 VOICE > Phone Book > Speed Dial

LABEL	DESCRIPTION
Destination	This indicates if the speed-dial entry uses one of your SIP accounts or uses the IP address or domain name of the SIP server.
Action	Click the Delete icon to erase this speed-dial entry.
Clear	Click to clear all fields on the screen and begin anew.
Reset	Click to restore your previously saved settings.

12.3.1 Speed Dial Setup

Click the **Edit** icon of an entry in the **VOICE > Phone Book > Speed Dial** screen to open the following screen. Use this screen to configure a speed dial entry.

Figure 52 VOICE > Phone Book > Speed Dial > Edit

The following table describes the labels in this screen.

Table 49 VOICE > Phone Book > Speed Dial > Edit

LABEL	DESCRIPTION
Speed Dial Setup	
Active	Select this check box to enable speed dial.
Speed Dial Number	Select the speed-dial number you want to use for this phone number.
Original Phone Number	Enter the original phone number you want the MAX-207HW2R to call when you dial the speed-dial number.
Name (or Memo)	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.

Table 49 VOICE > Phone Book > Speed Dial > Edit

LABEL	DESCRIPTION
Connection Type	Select Use Proxy if you want to use one of your SIP accounts to call this phone number. Select Non-Proxy (Use IP or URL) if you want to use a different SIP server or if you want to make a peer-to-peer call. In this case, enter the IP address or domain name of the SIP server or the other party in the field below.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

The Certificates Screens

13.1 Overview

Use the **TOOLS > Certificates** screens to import/manage public key certificates on the MAX-207HW2R.

The MAX-207HW2R can use public key certificates (also sometimes called “digital IDs”) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions (to name a few) receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on his site to be issued to all visiting web browsers to let them know that the site is legitimate.

13.1.1 What You Can Do in This Chapter

- The **My Certificates** screen ([Section 13.2 on page 128](#)) lets you import the MAX-207HW2R’s CA-signed certificates.
- The **Trusted CAs** screen ([Section 13.3 on page 129](#)) lets you import trusted CA-signed certificates.

13.1.2 What You Need to Know

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

Certificate Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the MAX-207HW2R to generate certification requests that contain identifying

information and public keys and then send the certification requests to a certification authority.

13.2 My Certificates

Click **TOOLS > Certificates > My Certificates** to import a certificate that matches a corresponding certification request that was generated by the MAX-207HW2R. You must remove any spaces from the certificate's filename before you can import it.

Figure 53 TOOLS > Certificates > My Certificates

The following table describes the labels in this screen.

Table 50 TOOLS > Certificates > My Certificates

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the MAX-207HW2R.
Browse	Click to find the certificate file you want to upload.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

13.3 Trusted CAs

Click **TOOLS > Certificates > Trusted CAs** to open the following screen. Follow the instructions in this screen to save a trusted certification authority's certificate from a computer to the MAX-207HW2R. The MAX-207HW2R trusts any valid certificate signed by any of the imported trusted CA certificates.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 54 TOOLS > Certificates > Trusted CAs

The following table describes the labels in this screen.

Table 51 TOOLS > Certificates > Trusted CAs Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse...	Click to find the certificate file you want to upload.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

13.4 Technical Reference

The following section contains additional technical information about the MAX-207HW2R features described in this chapter.

13.4.1 Certificate Authorities

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as “digital signatures”). Only you can write your signature exactly as it ought to look. When people know what your signature ought to look like, they can verify whether something was signed by you, or by someone else. In the same way, your private key “writes” your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

- 1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
- 2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
- 3 Tim uses his private key to sign the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim’s public key to verify it. Jenny knows that the message is from Tim, and she knows that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim’s private key).
- 5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny’s public key to verify the message.

The MAX-207HW2R uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority’s public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The MAX-207HW2R does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The MAX-207HW2R can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

13.4.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The MAX-207HW2R only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

13.4.1.2 Self-signed Certificates

You can have the MAX-207HW2R act as a certification authority and sign its own certificates.

13.4.1.3 Factory Default Certificate

The MAX-207HW2R generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

13.4.1.4 Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The MAX-207HW2R currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

Note: Be careful to not convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

13.4.2 Verifying a Certificate

Before you import a certificate into the MAX-207HW2R, you should verify that you have the correct certificate. This is especially true of trusted certificates since the MAX-207HW2R also trusts any valid certificate signed by any of the imported trusted certificates.

13.4.2.1 Checking the Fingerprint of a Certificate on Your Computer

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

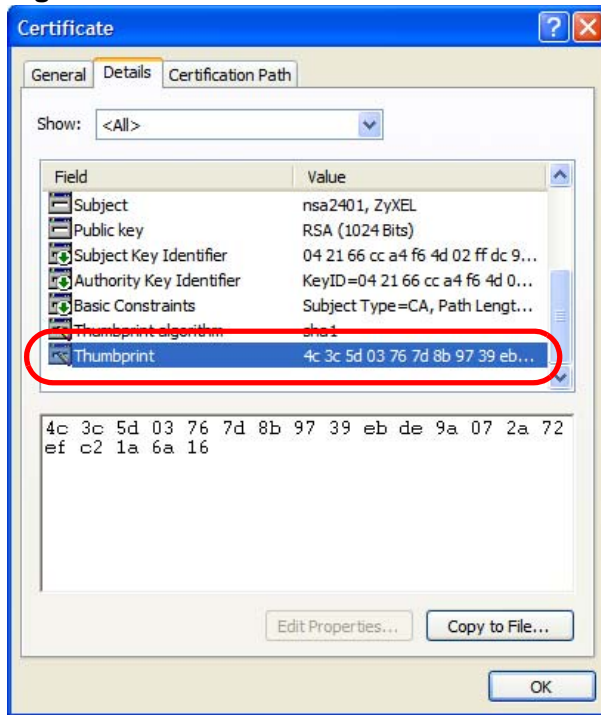
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension. (On some Linux distributions, the file extension may be ".der".)

Figure 55 Remote Host Certificates



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 56 Certificate Details



- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

The Remote Management Screens

14.1 Overview

Use the **TOOLS > Remote MGMT** screens to control which computers can use which services to access the MAX-207HW2R on each interface.

Remote management allows you to determine which services/protocols can access which MAX-207HW2R interface (if any) from which computers.

You may manage your MAX-207HW2R from a remote location via:

Table 52 Remote Management

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The MAX-207HW2R automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Telnet
- 2 HTTP

14.1.1 What You Can Do in This Chapter

- The **WWW** screen ([Section 14.2 on page 137](#)) lets you control HTTP access to your MAX-207HW2R.
- The **Telnet** screen ([Section 14.3 on page 138](#)) lets you control Telnet access to your MAX-207HW2R.
- The **FTP** screen ([Section 14.4 on page 139](#)) lets you control FTP access to your MAX-207HW2R.

- The **SNMP** screen ([Section 14.5 on page 140](#)) lets you control SNMP access to your MAX-207HW2R.
- The **DNS** screen ([Section 14.6 on page 143](#)) lets you control DNS access to your MAX-207HW2R.
- The **Ping** screen ([Section 14.7 on page 144](#)) lets you control how your MAX-207HW2R responds to other types of requests.

14.1.2 What You Need to Know

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

Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the MAX-207HW2R will disconnect the session immediately.
- 4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

Remote Management and NAT

When NAT is enabled:

- Use the MAX-207HW2R's WAN IP address when configuring from the WAN.
- Use the MAX-207HW2R's LAN IP address when configuring from the LAN.

System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The MAX-207HW2R automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the

TCP/IP protocol suite. Your MAX-207HW2R supports SNMP agent functionality, which allows a manager station to manage and monitor the MAX-207HW2R through the network. The MAX-207HW2R supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

14.2 WWW

Click **TOOLS > Remote MGMT > WWW** to control HTTP access to your MAX-207HW2R.

Figure 57 TOOLS > Remote MGMT > WWW

The following table describes the labels in this screen.

Table 53 TOOLS > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the MAX-207HW2R. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the MAX-207HW2R using this service.
Secured Client IP Address	Select All to allow any computer to access the MAX-207HW2R using this service. Select Selected to only allow the computer with the IP address that you specify to access the MAX-207HW2R using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

14.3 Telnet

Click **TOOLS > Remote MGMT > Telnet** to control Telnet access to your MAX-207HW2R.

Figure 58 TOOLS > Remote MGMT > Telnet

The following table describes the labels in this screen.

Table 54 TOOLS > Remote MGMT > Telnet

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the MAX-207HW2R. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the MAX-207HW2R using this service.
Secured Client IP Address	Select All to allow any computer to access the MAX-207HW2R using this service. Select Selected to only allow the computer with the IP address that you specify to access the MAX-207HW2R using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

14.4 FTP

Click **TOOLS > Remote MGMT > FTP** to control FTP access to your MAX-207HW2R.

Figure 59 TOOLS > Remote MGMT > FTP

The following table describes the labels in this screen.

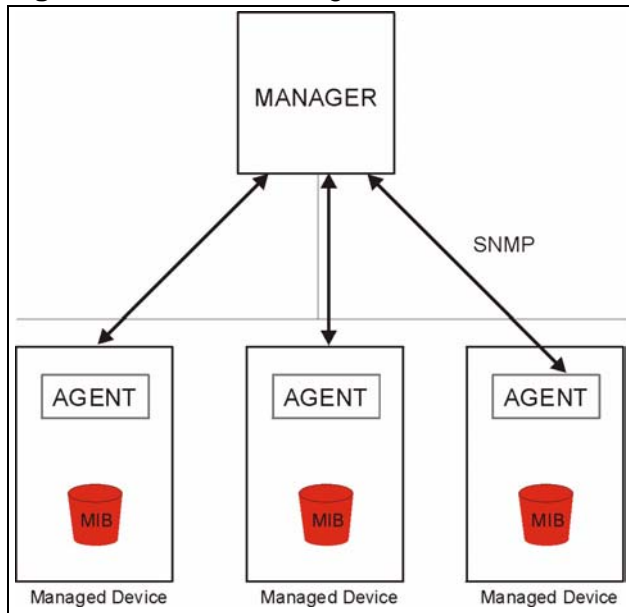
Table 55 TOOLS > Remote MGMT > FTP

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the MAX-207HW2R. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the MAX-207HW2R using this service.
Secured Client IP Address	Select All to allow any computer to access the MAX-207HW2R using this service. Select Selected to only allow the computer with the IP address that you specify to access the MAX-207HW2R using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

14.5 SNMP

An SNMP managed network consists of two main types of component: agents and a manager.

Figure 60 SNMP Management Model



An agent is a management software module that resides in a managed device (the MAX-207HW2R). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects. The MAX-207HW2R supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.

- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

14.5.1 SNMP Traps

The MAX-207HW2R sends traps to the SNMP manager when any of the following events occurs:

Table 56 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, C1 command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

14.5.2 SNMP Options

Click **TOOLS > Remote MGMT > SNMP** to control SNMP access to your MAX-207HW2R.

Figure 61 TOOLS > Remote MGMT > SNMP

The following table describes the labels in this screen.

Table 57 TOOLS > Remote MGMT > SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Enter the IP address of the station to send your SNMP traps to.
SNMP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the MAX-207HW2R using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the MAX-207HW2R using this service. Select All to allow any computer to access the MAX-207HW2R using this service. Choose Selected to just allow the computer with the IP address that you specify to access the MAX-207HW2R using this service.

Table 57 TOOLS > Remote MGMT > SNMP (continued)

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

14.6 DNS

Click **TOOLS > Remote MGMT > DNS** to control DNS access to your MAX-207HW2R.

Figure 62 TOOLS > Remote MGMT > DNS

The screenshot shows the DNS configuration interface. At the top, there are tabs for WWW, Telnet, FTP, SNMP, DNS, and Ping. The DNS tab is selected. Below the tabs, there are three main configuration sections:

- Server Port:** A text input field containing the number 53.
- Server Access:** A dropdown menu currently set to LAN.
- Secured Client IP Address:** Two radio buttons, 'All' (which is selected) and 'Selected'. To the right of the 'Selected' radio button is a text input field containing the IP address 192.168.1.33.

 At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 58 TOOLS > Remote MGMT > DNS

LABEL	DESCRIPTION
Server Port	This field is read-only. This field displays the port number this service uses to access the MAX-207HW2R. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the MAX-207HW2R using this service.
Secured Client IP Address	Select All to allow any computer to access the MAX-207HW2R using this service. Select Selected to only allow the computer with the IP address that you specify to access the MAX-207HW2R using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

14.7 Ping

Click **TOOLS > Remote MGMT > Ping** to control how your MAX-207HW2R responds to other types of requests.

Figure 63 TOOLS > Remote MGMT > Ping

The following table describes the labels in this screen.

Table 59 TOOLS > Remote MGMT > Security

LABEL	DESCRIPTION
Respond to Ping on	<p>Select the interface(s) on which the MAX-207HW2R should respond to incoming ping requests.</p> <ul style="list-style-type: none"> • LAN & WAN - the MAX-207HW2R responds to ping requests received from the LAN or the WAN. • Disable - the MAX-207HW2R does not respond to any ping requests. • LAN - the MAX-207HW2R only responds to ping requests received from the LAN. • WAN - the MAX-207HW2R only responds to ping requests received from the WAN.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

The Firewall Screens

15.1 Overview

Use the **TOOLS > Firewall** screens to manage MAX-207HW2R's firewall security measures.

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem.

A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

15.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 15.2 on page 146](#)) lets you configure the basic settings for your firewall.
- The **Services** screen ([Section 15.3 on page 149](#)) lets you enable service blocking, set up the date and time service blocking is effective, and to maintain the list of services you want to block.

15.1.2 What You Need to Know

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

About the MAX-207HW2R Firewall

The MAX-207HW2R firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The MAX-207HW2R's purpose is to allow a private Local Area Network (LAN) to be securely connected to

the Internet. The MAX-207HW2R can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The MAX-207HW2R is installed between the LAN and a WiMAX base station connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

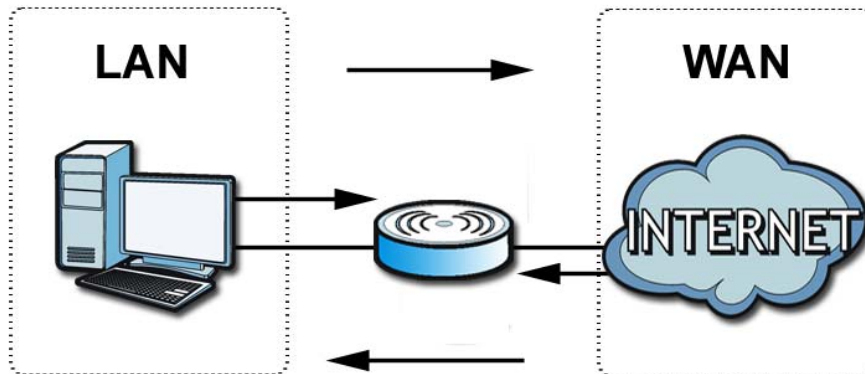
The MAX-207HW2R has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, “inbound access” is not allowed (by default) unless the remote host is authorized to use a specific service.

15.2 Firewall Setting

This section describes firewalls and the built-in MAX-207HW2R's firewall features.

15.2.1 Firewall Rule Directions

Figure 64 Firewall Rule Directions



LAN-to-WAN rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

You can block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are **LAN-to-WAN** firewall rules that block those services originating from the LAN.

Blocked **LAN-to-WAN** packets are considered alerts. Alerts are “higher priority logs” that include system errors, attacks and attempted access to blocked web sites. Alerts appear in red in the **View Log** screen. You may choose to have alerts e-mailed immediately in the **Log Settings** screen.

LAN-to-LAN/MAX-207HW2R means the LAN to the MAX-207HW2R LAN interface. This is always allowed, as this is how you manage the MAX-207HW2R from your local computer.

WAN-to-LAN rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by:

- Configuring NAT port forwarding rules.
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote MGMT** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/MAX-207HW2R firewall rules. WAN-to-WAN/MAX-207HW2R firewall rules are Internet to the MAX-207HW2R WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/MAX-207HW2R packets to log.

Forwarded **WAN-to-LAN** packets are not considered alerts.

15.2.2 Triangle Route

When the firewall is on, your MAX-207HW2R acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the MAX-207HW2R to protect your LAN against attacks.

Figure 65 Ideal Firewall Setup



15.2.3 Firewall Setting Options

Click **TOOLS > Firewall > General** to configure the basic settings for your firewall.

Figure 66 TOOLS > Firewall > General

The following table describes the labels in this screen.

Table 60 TOOLS > Firewall > General

LABEL	DESCRIPTION
Firewall Setup	
Enable Firewall	Select this to activate the firewall. The MAX-207HW2R controls access and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this if you want to let some traffic from the WAN go directly to a computer in the LAN without passing through the MAX-207HW2R.
Packet Direction	
Log	Select the situations in which you want to create log entries for firewall events. No Log - do not create any log entries Log Blocked - (LAN to WAN only) create log entries when packets are blocked Log All - create log entries for every packet
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

15.3 Services

Click **TOOLS > Firewall > Services** to enable service blocking, set up the date and time service blocking is effective, and to maintain the list of services you want to block.

Figure 67 TOOLS > Firewall > Service Setting

The following table describes the labels in this screen.

Table 61 TOOLS > Firewall > Service Setting

LABEL	DESCRIPTION
Service Setup	
Enable Services Blocking	Select this to activate service blocking. The Schedule to Block section controls what days and what times service blocking is actually effective, however.

Table 61 TOOLS > Firewall > Service Setting (continued)

LABEL	DESCRIPTION
Available Services	<p>This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click Add to add the port to the Blocked Services field.</p> <p>A custom port is a service that is not available in the pre-defined Available Services list. You must define it using the Type and Port Number fields.</p>
Blocked Services	<p>This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click Remove.</p>
Type	<p>Select TCP or UDP, based on which one the custom port uses.</p>
Port Number	<p>Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range of 6345-6349.</p>
Source IP	<p>You can configure the source addresses to which this firewall rule applies.</p> <p>Select Single IP from the drop-list to apply the firewall rule to packets with a particular (single) IP.</p> <p>Select Range IP to apply the firewall rule to packets within a range of IP addresses.</p> <p>If you do not want the firewall rule to apply to any IP address, select None.</p>
Destination IP	<p>You can configure the destination addresses or ranges of addresses to which this firewall rule applies.</p> <p>Select Single IP from the drop-list to apply the firewall rule to packets with a particular (single) IP.</p> <p>Select Range IP to apply the firewall rule to packets within a range of IP addresses.</p> <p>If you do not want the firewall rule to apply to any IP address, select None.</p>
Add	<p>Click this to add the selected service in Available Services to the Blocked Services list.</p>
Remove	<p>Select a service in the Blocked Services, and click this to remove the service from the list.</p>
Schedule to Block	
Enable Schedule	<p>Select this check box to enable your schedule for blocking.</p>
Day to Block	<p>Select which days of the week you want the service blocking to be effective.</p>
Time of Day to Block	<p>Select what time each day you want service blocking to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.</p>
Apply	<p>Click to save your changes.</p>
Reset	<p>Click to restore your previously saved settings.</p>