

# MAX208M2W Series

WiMAX Indoor VoIP Wi-Fi IAD

## User's Guide

### Default Login Details

IP Address: <http://192.168.1.1>

Admin's  
User Name and  
Password: admin / 1234

Guest's User  
Name and  
Password: guest / guest

Software Version 2.00  
Edition 1, 1/2011

[www.zyxel.com](http://www.zyxel.com)



# ZyXEL

Copyright © 2011  
ZyXEL Communications Corporation



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the ZyXEL MAX208M2W Series using the ZyXEL 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.
- Support Disc  
Refer to the included CD for support documents.
- ZyXEL Web Site  
Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## Documentation Feedback

Send your comments, questions or suggestions to: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.

## Need More Help?

More help is available at [www.zyxel.com](http://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 documentation 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](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 MAX208M2W Series.**

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





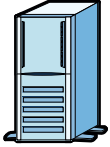






## Syntax Conventions

- The product(s) described in this book may be referred to as the "MAX208M2W Series", 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 MAX208M2W Series icon is not an exact representation of your product.

**Table 1** Common Icons

MAX208M2W Series 	Computer 	Wireless Signal 
Notebook 	Server 	Base Station 
Telephone 	Switch 	Router 
Internet Cloud 	Network Cloud 	

# Safety Warnings

**For your safety, be sure to read and follow all warning notices and instructions.**

- 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

<b>User's Guide .....</b>	<b>17</b>
Getting Started .....	19
Introducing the Web Configurator .....	25
Setup Wizard .....	31
Tutorials .....	43
<b>Technical Reference .....</b>	<b>63</b>
System Status .....	65
WiMAX .....	69
Network Setting .....	89
Security .....	127
The VoIP General Screens .....	133
The VoIP Account Screens .....	139
The VoIP Line Screens .....	157
Maintenance .....	161
Troubleshooting .....	187
Product Specifications .....	193



# Table of Contents

<b>About This User's Guide .....</b>	<b>3</b>
<b>Document Conventions.....</b>	<b>5</b>
<b>Safety Warnings.....</b>	<b>7</b>
<b>Contents Overview .....</b>	<b>9</b>
<b>Table of Contents.....</b>	<b>11</b>
<b>Part I: User's Guide.....</b>	<b>17</b>
<b>Chapter 1</b>	
<b>Getting Started .....</b>	<b>19</b>
1.1 About Your MAX208M2W Series .....	19
1.1.1 WiMAX Internet Access .....	19
1.1.2 Make Calls via Internet Telephony Service Provider .....	20
1.2 MAX208M2W Series Hardware .....	21
1.2.1 LEDs .....	21
1.3 Good Habits for Managing the MAX208M2W Series .....	22
<b>Chapter 2</b>	
<b>Introducing the Web Configurator .....</b>	<b>25</b>
2.1 Overview .....	25
2.1.1 Accessing the Web Configurator .....	25
2.1.2 The Reset Button .....	26
2.1.3 Saving and Canceling Changes .....	27
2.1.4 Working with Tables .....	27
2.2 The Main Screen .....	28
<b>Chapter 3</b>	
<b>Setup Wizard .....</b>	<b>31</b>
3.1 Overview .....	31
3.1.1 Welcome to the Setup Wizard .....	31
3.1.2 LAN Settings .....	33
3.1.3 WiMAX Frequency Settings .....	34
3.1.4 WiMAX Authentication Settings .....	36
3.1.5 VoIP Settings .....	38

3.1.6 WLAN Settings .....	39
3.1.7 Setup Complete .....	41
<b>Chapter 4</b>	
<b>Tutorials .....</b>	<b>43</b>
4.1 Overview .....	43
4.2 WiMAX Connection Settings .....	43
4.3 Configuring LAN DHCP .....	44
4.4 Changing Certificate .....	46
4.5 Blocking Web Access .....	47
4.6 Configuring the MAC Address Filter .....	48
4.7 Setting Up NAT Port Forwarding .....	50
4.8 Access the MAX208M2W Series Using DDNS .....	53
4.8.1 Registering a DDNS Account on <a href="http://www.dyndns.org">www.dyndns.org</a> .....	53
4.8.2 Configuring DDNS on Your MAX208M2W Series .....	54
4.8.3 Testing the DDNS Setting .....	54
4.9 Configuring Static Route for Routing to Another Network .....	54
4.10 Remotely Managing Your MAX208M2W Series .....	57
4.11 VLAN Configuration Example .....	58
<b>Part II: Technical Reference .....</b>	<b>63</b>
<b>Chapter 5</b>	
<b>System Status .....</b>	<b>65</b>
5.1 Overview .....	65
5.2 System Status .....	65
<b>Chapter 6</b>	
<b>WiMAX.....</b>	<b>69</b>
6.1 Overview .....	69
6.1.1 What You Need to Know .....	69
6.2 Connection Settings .....	73
6.3 Frequency Settings .....	75
6.4 Authentication Settings .....	78
6.5 Connect .....	81
6.6 Wide Scan .....	84
6.7 Link Status .....	85
6.8 Link Statistics .....	87
6.9 Connection Info .....	88
6.10 Service Flow .....	88

<b>Chapter 7</b>	
<b>Network Setting.....</b>	<b>89</b>
7.1 Overview .....	89
7.1.1 What You Need to Know .....	89
7.2 WAN .....	94
7.3 PPPoE .....	96
7.4 GRE .....	98
7.5 EtherIP .....	98
7.6 IP .....	99
7.7 DHCP .....	100
7.8 WLAN .....	102
7.9 WPS .....	104
7.10 MAC Address Filter .....	104
7.11 Static Route .....	106
7.12 Static Route Add .....	106
7.13 RIP .....	107
7.14 Port Forwarding .....	108
7.14.1 Port Forwarding Wizard .....	110
7.15 Port Trigger .....	111
7.15.1 Port Trigger Wizard .....	112
7.15.2 Trigger Port Forwarding Example .....	113
7.16 DMZ .....	114
7.17 ALG .....	115
7.18 UPnP .....	116
7.18.1 Installing UPnP in Windows XP .....	116
7.18.2 Web Configurator Easy Access .....	120
7.19 VLAN .....	122
7.20 DDNS .....	125
7.21 Content Filter .....	126
<b>Chapter 8</b>	
<b>Security.....</b>	<b>127</b>
8.1 Overview .....	127
8.1.1 What You Need to Know .....	127
8.2 IP Filter .....	128
8.3 MAC Filter .....	129
8.4 DDOS .....	130
<b>Chapter 9</b>	
<b>The VoIP General Screens .....</b>	<b>133</b>
9.1 VoIP Overview .....	133
9.1.1 What You Can Do in This Chapter .....	133
9.1.2 What You Need to Know .....	133

9.1.3 Before you Begin .....	135
9.2 Media .....	135
9.2.1 QoS .....	136
9.2.2 QoS Settings .....	137
9.3 Technical Reference .....	137
9.3.1 DSCP and Per-Hop Behavior .....	137
<b>Chapter 10</b>	
<b>The VoIP Account Screens .....</b>	<b>139</b>
10.1 Overview .....	139
10.1.1 What You Can Do in This Chapter .....	139
10.1.2 What You Need to Know .....	139
10.1.3 SIP User Agent .....	140
10.2 Status .....	144
10.3 Server .....	146
10.4 Feature .....	147
10.5 User .....	150
10.6 Dialing .....	152
10.7 Speed Dial .....	152
10.8 FAX .....	153
10.9 Technical Reference .....	154
10.9.1 SIP Call Progression .....	154
10.9.2 SIP Client Server .....	155
<b>Chapter 11</b>	
<b>The VoIP Line Screens .....</b>	<b>157</b>
11.1 Overview .....	157
11.1.1 What You Can Do in This Chapter .....	157
11.1.2 What You Need to Know .....	157
11.2 Phone .....	158
11.3 Voice .....	159
11.4 Profile .....	159
<b>Chapter 12</b>	
<b>Maintenance .....</b>	<b>161</b>
12.1 Overview .....	161
12.1.1 What You Need to Know .....	161
12.2 Password .....	168
12.3 HTTP .....	169
12.4 Telnet .....	170
12.5 SSH .....	170
12.6 SNMP .....	171
12.7 CWMP .....	172

---

12.8 OMA-DM .....	174
12.9 Date .....	176
12.10 Time Zone .....	177
12.11 Upgrade File .....	177
12.11.1 The Firmware Upload Process .....	178
12.12 Upgrade Link .....	179
12.13 CWMP Upgrade .....	179
12.14 Backup .....	180
12.15 Restore .....	181
12.15.1 The Restore Configuration Process .....	181
12.16 Factory Defaults .....	182
12.17 Log Setting .....	182
12.18 Log Display .....	183
12.19 Ping Test .....	184
12.20 Traceroute Test .....	184
12.21 About .....	185
12.22 Reboot .....	185
<b>Chapter 13</b>	
<b>Troubleshooting.....</b>	<b>187</b>
13.1 Power, Hardware Connections, and LEDs .....	187
13.2 MAX208M2W Series Access and Login .....	188
13.3 Internet Access .....	190
13.4 Reset the MAX208M2W Series to Its Factory Defaults .....	191
13.4.1 Pop-up Windows, JavaScript and Java Permissions .....	192
<b>Chapter 14</b>	
<b>Product Specifications .....</b>	<b>193</b>
14.1 Wall-Mounting .....	201
14.1.1 The Wall-Mounting Kit .....	201
14.1.2 Instructions .....	201
Appendix A WiMAX Security .....	205
Appendix B Setting Up Your Computer's IP Address .....	209
Appendix C Pop-up Windows, JavaScript and Java Permissions.....	237
Appendix D IP Addresses and Subnetting .....	247
Appendix E Importing Certificates .....	259
Appendix F Common Services.....	291
Appendix G Legal Information.....	295

**Index.....299**



---

# **PART I**

## **User's Guide**

---



# 1

## Getting Started

### 1.1 About Your MAX208M2W Series

The MAX208M2W Series includes MAX208M2W and MAX218M2W.

The MAX208M2W Series has a built-in switch and two phone ports. 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 MAX208M2W Series's Voice over IP (VoIP) communication capabilities.

Additionally, The web browser-based Graphical User Interface (GUI), also known as the web configurator, provides easy management of the device and its features.

See [Chapter 14 on page 193](#) for a complete list of features for your model.

#### 1.1.1 WiMAX Internet Access

Connect your computer or network to the MAX208M2W Series for WiMAX Internet access. See the Quick Start Guide for instructions on hardware connection.

In a wireless metropolitan area network (MAN), the MAX208M2W Series connects to a WiMAX base station (BS) for Internet access.

The following diagram shows a notebook computer equipped with the MAX208M2W Series 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 MAX208M2W Series to make and receive the following types of VoIP telephone calls:

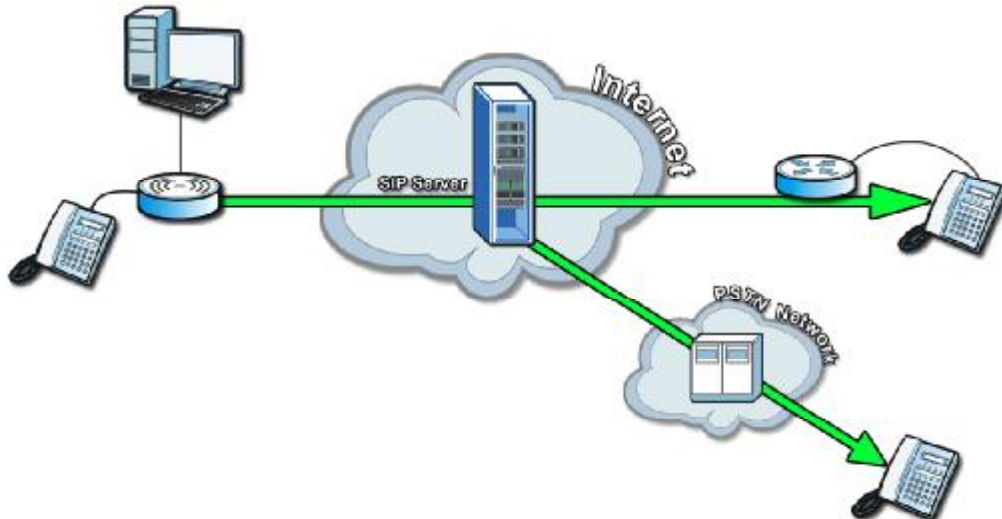
- Peer-to-Peer calls - Use the MAX208M2W Series to make a call directly to the recipient's IP address without using a SIP proxy server.

**Figure 2** VoIP Features - Peer-to-Peer Calls



- Calls via a VoIP service provider - The MAX208M2W Series sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

**Figure 3** Calls via VoIP Service Provider



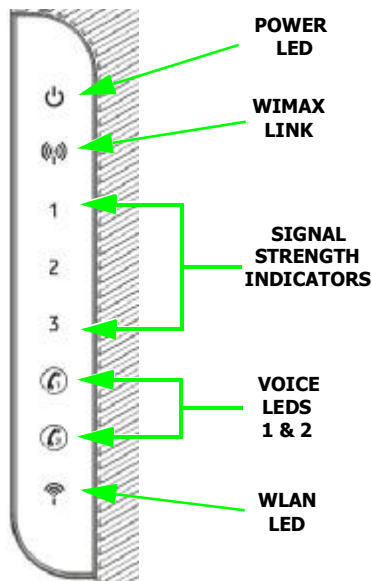
## 1.2 MAX208M2W Series Hardware

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 MAX208M2W Series.

**Figure 4** The MAX208M2W Series's LEDs



The following table describes your MAX208M2W Series's LEDs (from top to bottom).

**Table 2** The MAX208M2W Series LEDs behavior

LED	STATE	DESCRIPTION
Power	Off	The MAX208M2W Series is not receiving power.
	Red	The MAX208M2W Series 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	<b>Solid:</b> The MAX208M2W Series is receiving power and functioning correctly. <b>Flashing:</b> the device is self-testing (startup)

**Table 2** The MAX208M2W Series LEDs behavior

LED	STATE	DESCRIPTION
WiMAX Link	Off	The MAX208M2W Series is not connected to a wireless (WiMAX) network.
	Green	The MAX208M2W Series is successfully connected to a wireless (WiMAX) network.
	Green (Blinking Slowly)	The MAX208M2W Series is searching for a wireless (WiMAX) network.
	Green (Blinking Quickly)	The MAX208M2W Series has found a wireless (WiMAX) network and is connecting.
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 1 & 2	Off	No SIP account is registered, or the MAX208M2W Series is not receiving power.
	Green	A SIP account is registered.
	Green (Blinking)	A SIP account is registered, and the phone attached to the VoIP 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 VoIP 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 MAX208M2W Series

Do the following things regularly to make the MAX208M2W Series more secure and to manage the MAX208M2W Series 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 MAX208M2W Series becomes unstable or even crashes. If you forget your password, you will have to reset the MAX208M2W Series to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the MAX208M2W Series. 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).

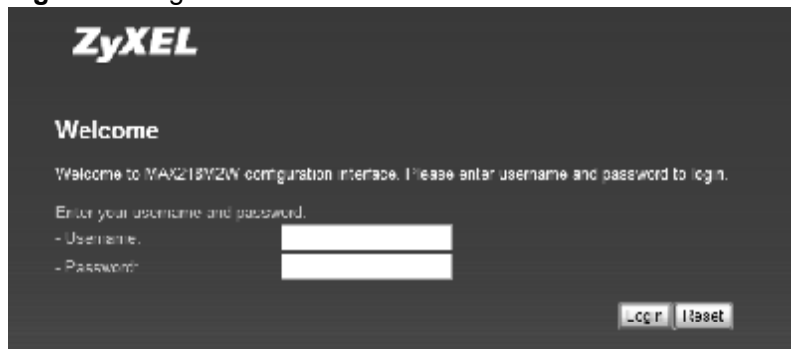
See the [Appendix C on page 237](#) for more information on configuring your web browser.

### 2.1.1 Accessing the Web Configurator

- 1 Make sure your MAX208M2W Series 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 **Username** (admin) and **Password** (1234), then click **Login**.

**Figure 5** Login screen



Note: For security reasons, the MAX208M2W Series automatically logs you out if you do not use the Web Configurator for five minutes. If this happens, log in again.

## 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 five seconds or until all LED lights blink one time, then release it. The device restarts when the defaults have been restored.
- 3 Reconfigure the MAX208M2W Series following the steps in your Quick Start Guide.

## 2.1.3 Saving and Canceling Changes

All screens to which you can make configuration changes must be saved before those changes can go into effect. If you make a mistake while configuring the MAX208M2W Series, you can cancel those changes and start over.

**Figure 6** Saving and Canceling Changes

**Wide Scan Result**

#	Frequency (KHz)	Bandwidth (MHz)
Total Num: 0		Search Clear

This screen contains the following fields:

**Table 3** Saving and Canceling Changes

LABEL	DESCRIPTION
Save	Click this to save your changes.
Cancel	Click this to restore the settings on this page to their last saved values.

Note: If you make changes to a page but do not save before switching to another page or exiting the Web Configurator, those changes are discarded.

## 2.1.4 Working with Tables

Many screens in the MAX208M2W Series contain tables to provide information or additional configuration options.

**Figure 7** Tables Example

#	SFID	SF Status	SF Direction
Total Num: 0		10 per page	0 page

This screen contains the following fields:

**Table 4** Saving and Canceling Changes

LABEL	DESCRIPTION
10 per page	<b>Items per Page</b> This displays the number of items displayed per table page. Use the menu to change this value.
⏪	<b>First Page</b> Click this to go to the first page in the table.

**Table 4** Saving and Canceling Changes (continued)

LABEL	DESCRIPTION
◀	<b>Previous Page</b> Click this to go to the previous page in the table.
0 ▾ page	<b>Page Indicator / Jump to Page</b> This indicates which page is currently displayed in the table. Use the menu to jump to another page. You can only jump to other pages if those pages exist.
▶	<b>Next Page</b> Click this to go to the previous page in the table.
▶▶	<b>Last Page</b> Click this to go to the last page in the table.
#	This indicates an item's position in the table. It has no bearing on that item's importance or lack there of.
Total Num	This indicates the total number of items in the table, including items on pages that are not visible.

## 2.2 The Main Screen

When you first log into the Web Configurator, the Main screen appears. Here you can view a summary of your MAX208M2W Series's connection status. This is also the default "home" page for the 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.





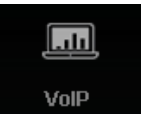
Note: The available menus and screens vary depending on the user account you use for login.

Figure 8 Main Screen


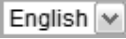




The following table describes the icons in this screen.

Table 5 Main &gt; Icons

ICON	DESCRIPTION
	System Status Click this to open the Main screen, which shows your MAX208M2W Series status and other information.
	WiMAX Click this to open the WiMAX menu, which gives you options for configuring your WiMAX settings.
	Network Setting Click this to open the Network menu, which gives you options for configuring your network settings.
	Security Click this to open the Security menu, which gives you options for configuring your firewall and security settings.
	VoIP Click this icon to open the VoIP menu, which gives you options on how to use the device to make phone calls.

**Table 5** Main > Icons (continued)

ICON	DESCRIPTION
	<p>Maintenance</p> <p>Click this to open the Maintenance menu, which gives you options for maintaining your MAX208M2W Series and performing basic network connectivity tests.</p>
	<p>Language</p> <p>Use this menu to select the Web Configurator's language.</p>
	<p>Setup Wizard</p> <p>Click this to open the Setup Wizard, where you can configure the most essential settings for your MAX208M2W Series to work.</p>
	<p>Logout</p> <p>Click this to log out of the Web Configurator.</p>

# 3

## Setup Wizard

### 3.1 Overview

This chapter provides information on the ZyXEL Setup Wizard. The wizard guides you through several steps for onfiguring your network settings.

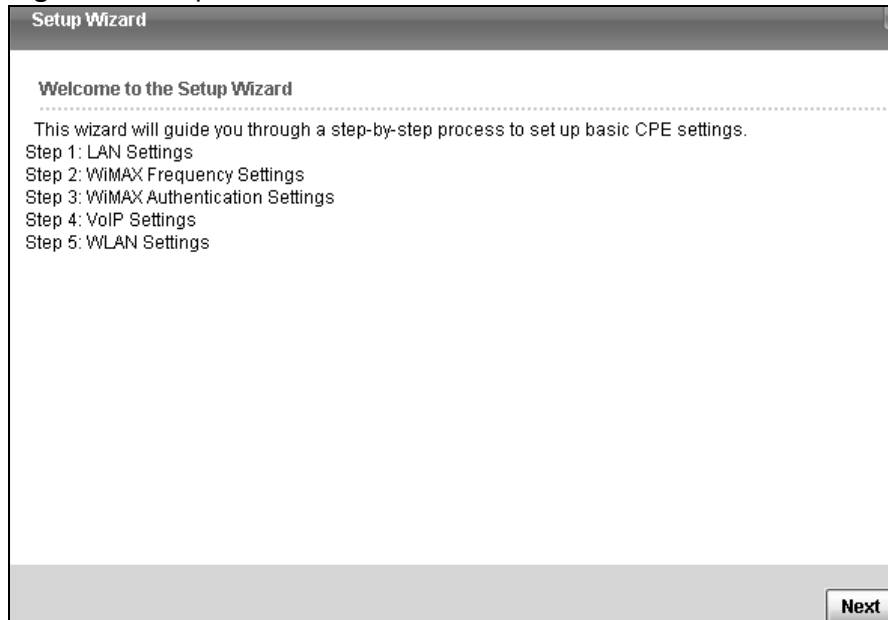
#### 3.1.1 Welcome to the Setup Wizard

This screen provides a quick summary of the configuration tasks the wizard helps you to perform. They are:

- 1 Set up your Local Area Network (LAN) options, which determine how the devices in your home or office connect to the MAX208M2W Series.
- 2 Set up your MAX208M2W Series's broadcast frequency, which is the radio channel it uses to communicate with the ISP's base station.
- 3 Set up your MAX208M2W Series's login options, which are used to connect your LAN to the ISP's network and verify your account.
- 4 Set up your MAX208M2W Series's VoIP Settings, which will allow you to make calls over the Internet.

- 5 Set up your MAX208M2W Series's WLAN so that other devices, such as a laptop or a smartphone, can connect wirelessly to the Internet using the MAX208M2W Series.

**Figure 9** Setup Wizard > Welcome





### 3.1.2 LAN Settings

The LAN Settings screen allows you to configure your local network options.

**Figure 10** Setup Wizard > LAN Settings

The following table describes the labels in this screen.

**Table 6** Setup Wizard > LAN Settings

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the IP address of the MAX208M2W Series on the LAN.  Note: This field is the IP address you use to access the MAX208M2W Series 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. 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.
DHCP Server	
Enable	Select this if you want the MAX208M2W Series to be the DHCP server on the LAN. As a DHCP server, the MAX208M2W Series assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information.
Start IP	Enter the IP address from which the MAX208M2W Series begins allocating IP addresses.
End IP	Enter the IP address at which the MAX208M2W Series stops allocating IP addresses.

**Table 6** Setup Wizard > LAN Settings (continued)

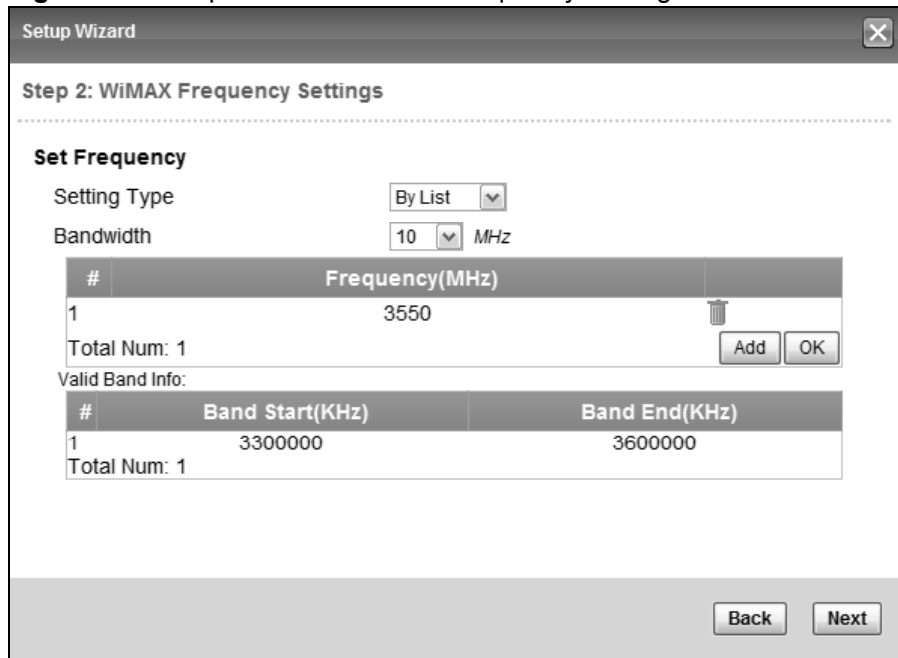
LABEL	DESCRIPTION
Lease Time	Enter the duration in minutes before the device requests a new IP address from the DHCP server.
DNS Server assigned by DHCP Server	
First DNS Server	Specify the first IP address of three DNS servers that the network can use. The MAX208M2W Series provides these IP addresses to DHCP clients.
Second DNS Server	Specify the second IP address of three DNS servers that the network can use. The MAX208M2W Series provides these IP addresses to DHCP clients.
Third DNS Server	Specify the third IP address of three DNS servers that the network can use. The MAX208M2W Series provides these IP addresses to DHCP clients.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

### 3.1.3 WiMAX Frequency Settings

The WiMAX Frequency Settings screen allows you to configure the broadcast radio frequency used by the MAX208M2W Series.

Note: These settings should be provided by your ISP.

**Figure 11** Setup Wizard > WiMAX Frequency Settings



The following table describes the labels in this screen.

**Table 7** Setup Wizard > WiMAX Frequency Settings

LABEL	DESCRIPTION
Setting Type	Select the WiMAX frequency setting type from the list. <ul style="list-style-type: none"> <li>• <b>By Range</b> - Select this to set up the frequency based on a range of MHz.</li> <li>• <b>By List</b> - Select this to set up the frequency on an individual MHz basis. You can add multiple MHz values to the list.</li> </ul>
Step	Enter the increments in MHz by which to increase the frequency range.  Note: This field only appears when you select <b>By Range</b> under <b>Setting Type</b> .
Start Frequency	Enter the frequency value at the beginning of the frequency range to use. The frequency is increased in increments equal to the <b>Step</b> value until the <b>End Frequency</b> is reached, at which time the cycle starts over with the <b>Start Frequency</b> .  Note: This field only appears when you select <b>By Range</b> under <b>Setting Type</b> .
End Frequency	Enter the frequency value at the end of the frequency range to use.  Note: This field only appears when you select <b>By Range</b> under <b>Setting Type</b> .
Bandwidth	Set the frequency bandwidth in MHz that this MAX208M2W Series uses.
#	This is an index number for enumeration purposes only.
Frequency (MHz)	Displays the frequency MHz for the item in the list.
Total Num	Displays the total number of items in the list.
Delete	Click this to remove an item from the list.
Add	Click this to add an item to the list.
OK	Click this to save an newly added item to the list.
#	This is an index number for enumeration purposes only.
Band Start (KHz)	Indicates the beginning of the frequency band in KHz.
Band End (KHz)	Indicates the end of the frequency band in KHz.
Total Num	Displays the total number of items in the list.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

### 3.1.4 WiMAX Authentication Settings

The WiMAX Authentication Settings screen allows you to configure how your MAX208M2W Series logs into the service provider’s network.

Note: These settings should be provided by your ISP.

Note: The EAP supplicant settings on this screen vary depending on the authentication mode you select.

**Figure 12** Setup Wizard > WiMAX Authentication Settings

**Step 3: WiMAX Authentication Settings**

**Authentication**

Authentication Mode: User and device authentication

**EAP Supplicant**

EAP Mode: EAP-TTLS

Anonymous ID: [Empty text box]

Ignore Cert Verification:

Server Root CA Cert. File: [Empty text box] Browse...

Server Root CA Cert. Info: No certificate file found

Device Cert. File: [Empty text box] Browse...

Device Cert. Info: No certificate file found

Device Private Key: [Empty text box] Browse...

Device Private Key Info: No private key found

Device Private Key Password: [Password field with 4 dots]

Inner Mode: MS-CHAPv2

Username: [Empty text box]

Password: [Password field with 4 dots]

Back Next

The following table describes the labels in this screen.

**Table 8** Setup Wizard > WiMAX Authentication Settings

LABEL	DESCRIPTION
Authentication	
Authentication Mode	Select a WiMAX authentication mode for authentication network sessions with the ISP. Options are: <ul style="list-style-type: none"> <li>No authentication</li> <li>User authentication</li> <li>Device authentication</li> <li>User and Device authentication</li> </ul>
EAP Supplication	
EAP Mode	Select an EAP authentication mode. See <a href="#">Table 15 on page 79</a> if you need more information.
Anonymous Id	Enter your anonymous ID.  Note: Some modes may not require this.
Ignore Cert Verification	Select this to ignore base station certification verification when a certificate is received during EAP-TLS or EAP-TTLS.
Server Root CA Cert. File	Browse for and choose a server root certificate file, if required.
Server Root CA Cert. Info	This field displays information about the assigned server root certificate.
Device Cert. File	Browse for and choose a device certificate file, if required.
Device Cert. Info.	This field displays information about the assigned device certificate.
Device Private Key	Browse for and choose a device private key, if required.
Device Private Key Info	This field displays information about the assigned device private key.
Device Private Key Password	Enter the device private key, if required.
Inner Mode	Select an inner authentication mode (MS-CHAP, MS-CHAPV2, CHAP, MD5, PAP. See <a href="#">Table 15 on page 79</a> if you need more information.
Username	Enter your authentication username.
Password	Enter your authentication password.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

### 3.1.5 VoIP Settings

The VoIP Settings screen allows you to configure how your MAX208M2W Series connects to up to two VoIP service providers' network and makes calls over the Internet.

Note: This settings should be provided by your VoIP service provider.

**Figure 13** Setup Wizard > VoIP Settings

**Step 4: VoIP Settings**

**Line 1 SIP Account**

Enable

SIP Server

Port Number

Subscriber Number

Display Name  *max*  
*length:64 characters*

Authentication Name

Password

**Line 2 SIP Account**

Enable

SIP Server

Port Number

Subscriber Number

Display Name  *max*  
*length:64 characters*

Authentication Name

Password

**Back** **Next**

The following table describes the labels in this screen.

**Table 9** Setup Wizard > VoIP Settings

LABEL	DESCRIPTION
Line 1 SIP Account	Configure this section to use the <b>PHONE 1</b> port.
Enable	Select this to activate the SIP account.
SIP Server	Enter the IP address or domain name of the SIP server.
Port Number	Enter the SIP server's listening port number.

**Table 9** Setup Wizard > VoIP Settings (continued)

LABEL	DESCRIPTION
Subscriber Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol.
Display Name	Enter the name that appears on the other party's device if they have Caller ID enabled.
Authentication Name	Type the SIP user name associated with this account for authentication to the SIP server.
Password	Type the SIP password associated with this account.
Line 2 SIP Account - Configure this section to use the <b>PHONE 2</b> port. See the fields above for similar description.	
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

### 3.1.6 WLAN Settings

The WLAN Settings screen lets you set up how other devices connect to the Internet wirelessly using the MAX208M2W Series.

**Figure 14** Setup Wizard > WLAN Settings

Setup Wizard

Step 5: WLAN Settings

**WiFi Settings**

Enable WLAN

WLAN Mode 802.11 B/G/N mixed

WLAN Channel channel 11

**SSID Settings**

WLAN SSID ZyXEL1

Hide SSID

Encryption Type WEP

**SSID WEP Settings**

Authentication Method OPEN SYSTEM

WEP Encryption Length 64-bit

Key 1 HEX \*\*\*\*\*

Key 2 HEX \*\*\*\*\*

Key 3 HEX \*\*\*\*\*

Key 4 HEX \*\*\*\*\*

Back Next

**Figure 15** Steup Wizard > WLAN Settings > Encryption Type: WPA Personal

SSID WPA Settings	
WPA Mode	WPA <input type="button" value="v"/>
Cipher Type	TKIP <input type="button" value="v"/>
Pre-shared Key	*****

The following table describes the labels in this screen.

**Table 10** Setup Wizard > WLAN Settings

LABEL	DESCRIPTION
Wifi Settings	
Enable WLAN	Select this box to enable the wireless service and allow other wireless clients to connect to the Internet using the MAX208M2W Series.
WLAN Mode	Select the mode that the MAX208M2W Series will be using to communicate: 802.11 B/G/N mixed, 802.11 B/G mixed, 802.11 B only, 802.11 G only, or 802.11 N only.
WLAN Channel	Select one channel from 1 to 13 for wireless communications with the wireless stations.
SSID Settings	
WLAN SSID	This field dilsplays the name of the wireless network associated with the MAX208M2W Series.
Hide SSID	Select this option if you wish to keep the name of the wireless network hidden.
Encryption Type	Select the type of encryption that the network will be using: None, WEP, or WPA Personal.
SSID WEP Settings	
Note: You will only see this options if you selected WEP as the Encryption Type.	
Authentication Method	Select the type of authentication used to join the network: Openn System or Shared Key.
WEP Encryption Length	Select the length of the encryption key: 64-bit or 128-bit.
Key 1 - 4	Pick one of four available keys. The key can be in either Hexagecimal (HEX) or ASCII format.  Type the key using any letters and numbers. The field is case sensitive and the lenght must match the length picked in the step above (64-bit or 128-bit). A warning mesage will appear if you fail to do this.
SSID WPA Settings	

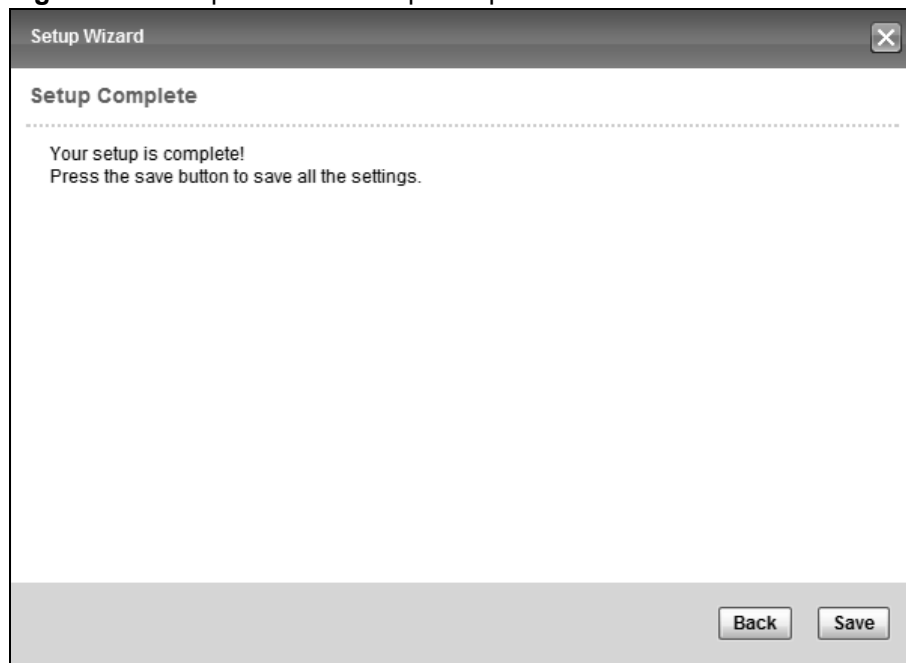


**Table 10** Setup Wizard > WLAN Settings (continued)

LABEL	DESCRIPTION
WPA Mode	Select either WPA, WPA2 or Auto (WPA or WPA2).
Cipher Type	Select the type of authentication that you wish to use for your network: TKIP, AES or both. AES is more secure.
Pre Shared Key	Type the pre-shared key or PSK previously shared between the two parties.

### 3.1.7 Setup Complete

Click **Save** to save the Setup Wizard settings and close it.

**Figure 16** Setup Wizard > Setup Complete

Launch your web browser and navigate to [www.zyxel.com](http://www.zyxel.com). If everything was configured properly, the web page should display. You can now surf the Internet!

Refer to the rest of this guide for more detailed information on the complete range of MAX208M2W Series features available in the more advanced web configurator.

Note: If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.



# 4

## Tutorials

### 4.1 Overview

This chapter shows you how to configure some of the MAX208M2W Series's features.

Note: Be sure to read [Introducing the Web Configurator on page 25](#) before working through the tutorials presented here. For field descriptions for individual screens, see the related technical reference in this User's Guide.

This chapter includes the following configuration examples:

- [WiMAX Connection Settings on page 43](#)
- [Configuring LAN DHCP on page 44](#)
- [Changing Certificate on page 46](#)
- [Blocking Web Access on page 47](#)
- [Configuring the MAC Address Filter, see page 48](#)
- [Setting Up NAT Port Forwarding, see page 50](#)
- [Access the MAX208M2W Series Using DDNS, see page 53](#)
- [Configuring Static Route for Routing to Another Network, see page 54](#)
- [Remotely Managing Your MAX208M2W Series on page 57](#)
- [VLAN Configuration Example on page 58](#)

### 4.2 WiMAX Connection Settings

This tutorial provides you with pointers for configuring the MAX208M2W Series to connect to an ISP.

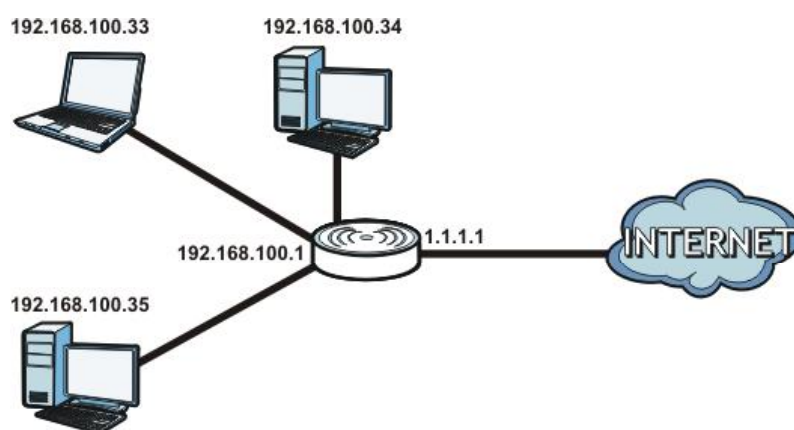
- 1 Connect the MAX208M2W Series to the ISP's nearest base station. See [Section 6.2 on page 73](#).
- 2 Configure the MAX208M2W Series's broadcast frequency. [Section 6.3 on page 75](#).

- 3 Configure the MAX208M2W Series to connect securely to the ISP's authentication servers. See [Section 6.4 on page 78](#).
- 4 Check the MAX208M2W Series's connection status to ensure everything is working properly. See [Section 6.7 on page 85](#).

## 4.3 Configuring LAN DHCP

This tutorial shows you how to set up a small network in your office or home.

**Goal:** Connect three computers to your MAX208M2W Series to form a small network.



**Required:** The following table provides a summary of the information you will need to complete the tasks in this tutorial.

INFORMATION	VALUE	SEE ALSO
LAN IP Address	192.168.100.1	<a href="#">Chapter 7 on page 99</a>
Starting IP Address	192.168.100.10	<a href="#">Chapter 7 on page 100</a>
Ending IP Address	192.168.100.30	
DNS Servers	From ISP	

- 1 In the Web Configurator, open the **Networking Setting > LAN** screen and set the IP Address to 192.168.100.1. Use the default **IP Subnet Mask** of 255.255.255.0. Click **Save**.

IP Address

IP Subnet Mask

- 2 Manually change the IP address of your computer that you are using to 192.168.100.x (for example, 192.168.100.5) and keep the subnet set to 255.255.255.0.
- 3 Type <http://192.168.100.1> in your browser after the MAX208M2W Series finishes starting up completely.
- 4 Log into the Web Configurator and open the **Networking Setting > LAN > DHCP** screen.

- 5 Select **Server** for the DHCP mode, then enter 192.168.100.10 and 192.168.100.30 as your DHCP starting and ending IP addresses.
- 6 Leave the other settings as their defaults and click **Save**.
- 7 Next, go to the **Networking Setting > WAN** screen and select **NAT** in the **Operation Mode** field. Click **Save**.

- 8 Connect your computers to the MAX208M2W Series's Ethernet ports and you're all set!

Note: You may need to configure the computers on your LAN to automatically obtain IP addresses. For information on how to do this, see [Appendix B on page 209](#).

Once your network is configured and hooked up, you will want to connect it to the Internet next. To do this, just run the **Internet Connection Wizard** ([Chapter 3 on page 31](#)), which walks you through the process.

## 4.4 Changing Certificate

This tutorial shows you how to import a new security certificate, which allows your device to communicate with another network servers.

**Goal:** Import a new security certificate into the MAX208M2W Series.

**See Also:** [Appendix E on page 259](#).

- 1 Go to the **WiMAX > Profile > Authentication Settings** screen. In the **EAP Supplicant** section, click each **Browse** button and locate the security certificates that were provided by your new ISP.

- 2 Configure your new Internet access settings based on the information provided by the ISP.

Note: You can also use the Internet Connection Wizard to configure the Internet access settings.

- 3 You may need to configure the **Options** section according to the information provided by the ISP.

Options	
Enable Auth Mode Decoration In	<input type="checkbox"/>
EAP Outer ID	
Enable Service Mode Decoration In	<input type="checkbox"/>
EAP Outer ID	
Random Outer ID	<input type="checkbox"/>
Ignore Cert Verification	<input type="checkbox"/>
Same EAP OuterID in ReAuth	<input type="checkbox"/>
MAC address in RADIUS Spouter ID	<input type="checkbox"/>
Delete existed Root Certificate file	<input type="checkbox"/>
Delete existed Device Certificate file	<input type="checkbox"/>
Delete existed Private Key	<input type="checkbox"/>

- 4 Click **Save**. You should now be able to connect to the Internet through your new service provider!

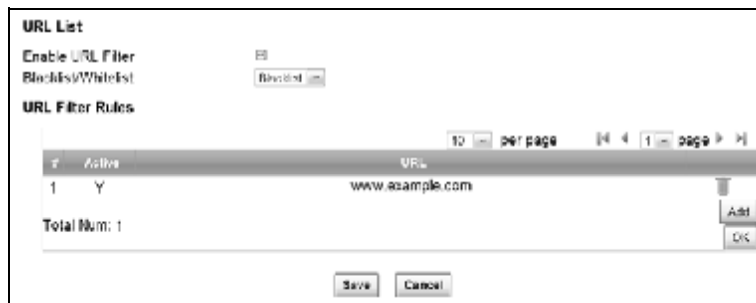
## 4.5 Blocking Web Access

If your MAX208M2W Series is in a home or office environment you may decide that you want to block an Internet website access. You may need to block both the website's IP address and domain name.

**Goal:** Configure the MAX208M2W Series's content filter to block a website with a domain name [www.example.com](http://www.example.com).

**See Also:** [Section 7.21 on page 126](#).

- 1 Open the **Networking Setting > Content Filter**.
- 2 Select **Enable URL Filter**.
- 3 Select **Blacklist**.
- 4 Click **Add** and configure a URL filter rule by selecting **Active** and entering [www.example.com](http://www.example.com) as the URL.
- 5 Click **OK**.

**6 Click Save.**

Open a browser from your computer in the MAX208M2W Series's LAN network, you should get an "**Access Violation**" message when you try to access to <http://www.example.com>. You may also need to block the IP address of the website if you do not want users to access to the website through its IP address.

## 4.6 Configuring the MAC Address Filter

This tutorial shows you how to use the MAC filter to block a DHCP client's access to hosts and to the WiMAX network.



- 1 First of all, you have to know the MAC address of the computer. If not, you can look for the MAC address in the **Network Setting > LAN > DHCP** screen. (192.168.100.3 mapping to 00:02:E3:53:16:95 in this example).

**DHCP Server**

DHCP Mode: Server

Start IP: 192.168.100.2

End IP: 192.168.100.254

Lease Time: 1440 minutes

Relay IP: 0.0.0.0

**DNS Server assigned by DHCP Server**

First DNS Server: From ISP 0.0.0.0

Second DNS Server: From ISP 0.0.0.0

Third DNS Server: From ISP 0.0.0.0

**Static DHCP**

#	MAC Address	IP Address
Total Num: 0		

**DHCP Leased Hosts**

#	MAC Address	IP Address	Remaining Time
1	00:02:E3:53:16:95	192.168.100.2	23:57:44
2	00:02:E3:53:16:95	192.168.100.3	23:57:30
Total Num: 2			

Save Cancel

- 2 Click **Security > Firewall > MAC Filter**. Select **Blacklist** and click the **Add** button in the **MAC Filter Rules** table.

**MAC List**

Blacklist/Whitelist: Blacklist

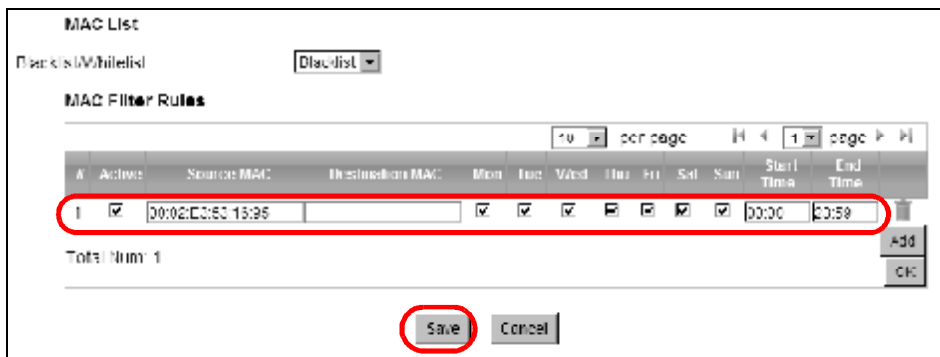
**MAC Filter Rules**

#	Active	Source MAC	Destination MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start time	End time
Total Num: 0												

Add

Save Cancel

- An empty entry appears. Enter the computer's MAC address in the **Source MAC** field and leave the other fields set to their defaults. Click **Save**.



The computer will no longer be able to access any host on the WiMAX network through the MAX208M2W Series.

## 4.7 Setting Up NAT Port Forwarding

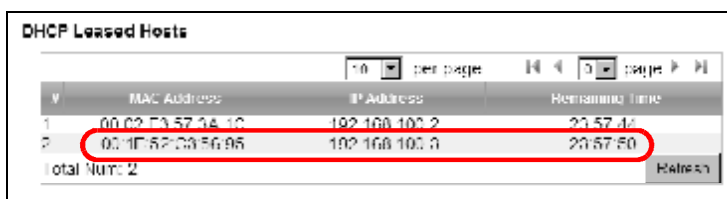
Thomas recently received an Xbox 360 as his birthday gift. His friends invited him to play online games with them on Xbox LIVE. In order to communicate and play with other gamers on Xbox LIVE, Thomas needs to configure the port settings on his MAX208M2W Series.

Xbox 360 requires the following ports to be available in order to operate Xbox LIVE correctly:

TCP: 53, 80, 3074

UDP: 53, 88, 3074

- You have to know the Xbox 360's IP address first. You can check it through the Xbox 360 console. You may be able to check the IP address on the MAX208M2W Series if the MAX208M2W Series has assigned a DHCP IP address to the Xbox 360. Check the **DHCP Leased Hosts** table in the **Network > LAN > DHCP** screen. Look for the IP address for the Xbox 360.



- 2 NAT mode is required to use port forwarding. Click **Network Setting** > **WAN** and make sure **NAT** is selected in the **Operation Mode** field. Click **Save**.

The screenshot shows the WAN configuration interface. The 'Operation Mode' dropdown menu is highlighted with a red circle and set to 'NAT'. Other fields include WAN Protocol (Ethernet), Bridging LAN ARP (No), Get IP Method (From ISP), WAN IP Request Timeout (120), WAN IP Address (0.0.0.0), WAN IP Subnet Mask (0.0.0.0), Gateway IP Address (0.0.0.0), MTU (1400), and Clone MAC Address (0000-22-00-00-00-00). Under the 'WAN DNS' section, there are three fields for First, Second, and Third DNS Servers, all set to 'From ISP' and '0.0.0.0'. 'Save' and 'Cancel' buttons are at the bottom.

- 3 Click **Network Setting** > **NAT** > **Port Forwarding** and then click the first entry to edit the rule.

The screenshot shows the Port Forwarding table. The first entry is selected and highlighted with a red circle. The table has columns for #, Active, Name, Protocol, Incoming Port(s) (Start Port, End Port), Forward Port(s) (Start Port, End Port), and Server IP. The first entry has Name1, TCP, 0-0, 0-0, and Server IP 1.1.1.1. 'Save' and 'Cancel' buttons are at the bottom.

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP
				Start Port	End Port	Start Port	End Port	
1	N	Name1	TCP	0	0	0	0	1.1.1.1
2	N	Name2	TCP	0	0	0	0	1.1.1.1
3	N	Name3	TCP	0	0	0	0	1.1.1.1
4	N	Name4	TCP	0	0	0	0	1.1.1.1
5	N	Name5	TCP	0	0	0	0	1.1.1.1

- 4 Configure the screen as follows to open TCP/UDP port 53 for the Xbox 360. Click **OK**.

The screenshot shows the Port Forwarding table with the first entry configured. The 'Active' checkbox is checked, the Name is 'Xbox360', the Protocol is 'TCP', and the Incoming and Forward ports are all set to '53'. The Server IP is '192.168.1.24'. 'Save' and 'Cancel' buttons are at the bottom.

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP
				Start Port	End Port	Start Port	End Port	
1	<input checked="" type="checkbox"/>	Xbox360	TCP	53	53	53	53	192.168.1.24
2	N	Name2	TCP	0	0	0	0	1.1.1.1
3	N	Name3	TCP	0	0	0	0	1.1.1.1
4	N	Name4	TCP	0	0	0	0	1.1.1.1
5	N	Name5	TCP	0	0	0	0	1.1.1.1

- Repeat steps 2 and 3 to open the rest of the ports for the Xbox 360. The port forwarding settings you configured are listed in the **Port Forwarding** screen.

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP*
				Start Port	End Port	Start Port	End Port	
1	Y	Xbox 360	UDP	13	68	68	13	192.168.1.34
2	Y	Xbox 360	UDP	80	80	80	80	192.168.1.34
3	Y	Xbox 360	TCP	88	88	88	88	192.168.1.34
4	Y	Xbox 360	UDP	3074	3074	3074	3074	192.168.1.34
5	N	Named	TCP	0	0	0	0	1.1.1.1

Total Num: 5

Buttons: Save, Cancel, Add, OK, Wlan

- Click **Save**.

Thomas can then connect his Xbox 360 to the Internet and play online games with his friends.

In this tutorial, all port 80 traffic is forwarded to the Xbox 360, but port 80 is also the default listening port for remote management via WWW. If Thomas also wants to manage the MAX208M2W Series from the Internet, he has to assign an unused port to WWW remote access.

Click **Advanced > Remote MGMT**. Enter an unused port in the **Port** field (81 in this example). Click **Save**.

**HTTP Server**

Enable

Port Number

**HTTPS Server**

Enable

Port Number

**HTTP and HTTPS**

Allow Connection from WAN

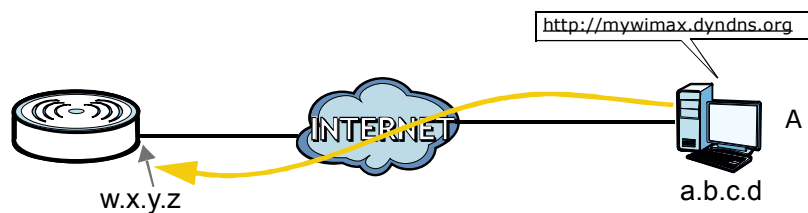
**HTTP Session Timeout**

Session Timeout  minutes (0-99, default 5, 0 means disabled)

Buttons: Save, Cancel

## 4.8 Access the MAX208M2W Series Using DDNS

If you connect your MAX208M2W Series to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The MAX208M2W Series's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the MAX208M2W Series using a domain name.



To use this feature, you have to apply for DDNS service at [www.dyndns.org](http://www.dyndns.org).

This tutorial covers:

- [Registering a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [Configuring DDNS on Your MAX208M2W Series](#)
- [Testing the DDNS Setting](#)

Note: If you have a private WAN IP address (see [Private IP Addresses on page 256](#)), then you cannot use DDNS.

### 4.8.1 Registering a DDNS Account on [www.dyndns.org](http://www.dyndns.org)

- 1 Open a browser and type **<http://www.dyndns.org>**.
- 2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
- 3 Log into [www.dyndns.org](http://www.dyndns.org) using your account.
- 4 Add a new DDNS host name. This tutorial uses the following settings as an example.
  - Hostname: **mywimax.dyndns.org**
  - Service Type: **Host with IP address**
  - IP Address: Enter the WAN IP address that your MAX208M2W Series is currently using. You can find the IP address on the MAX208M2W Series's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the MAX208M2W Series later.

## 4.8.2 Configuring DDNS on Your MAX208M2W Series

Configure the following settings in the **Network Setting > DDNS** screen.

- 1 Select **Enable Dynamic DNS**.
- 2 Select **dyndns.org** for the service provider.
- 3 Select **Dynamic** for the service type.
- 4 Type **mywimax.dyndns.org** in the **Domain Name** field.
- 5 Enter the user name (**UserName1**) and password (**12345**).
- 6 Select **WAN IP** for the IP update policy.
- 7 Click **Save**.

## 4.8.3 Testing the DDNS Setting

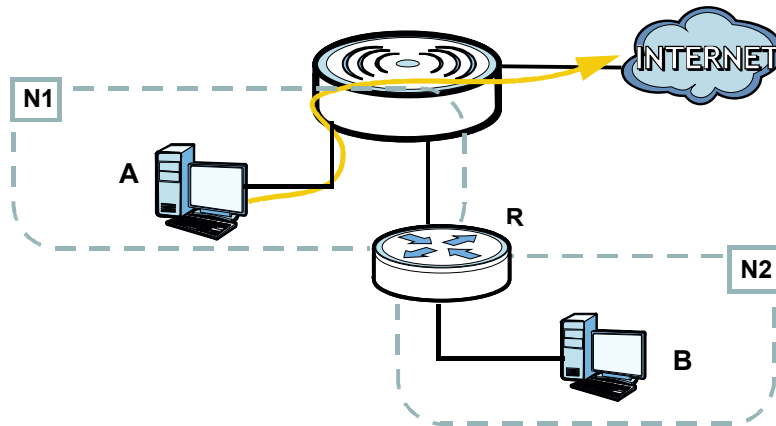
Now you should be able to access the MAX208M2W Series from the Internet. To test this:

- 1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
- 2 Type **http://mywimax.dyndns.org** and press [Enter].
- 3 The MAX208M2W Series's login page should appear. You can then log into the MAX208M2W Series and manage it.

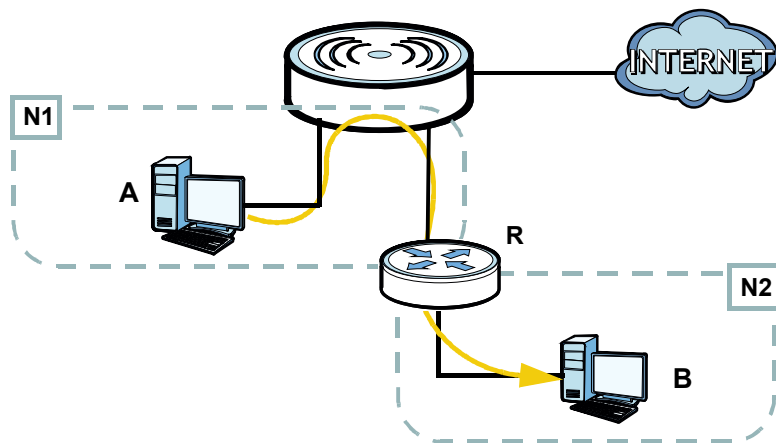
## 4.9 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the MAX208M2W Series's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the MAX208M2W Series's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the MAX208M2W Series's WAN default gateway by default. In this case, computer **B** will never receive the traffic.



You need to specify a static routing rule on the MAX208M2W Series to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the MAX208M2W Series routes traffic from computer **A** to **R** and then **R** routes the traffic to computer **B**.



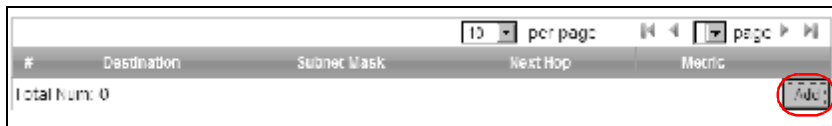
This tutorial uses the following example IP settings:

**Table 11** IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The MAX208M2W Series's WAN	172.16.1.1
The MAX208M2W Series's LAN	192.168.1.1
<b>A</b>	192.168.1.34
<b>R</b> 's IP address on N1	192.168.1.253
<b>R</b> 's IP address on N2	192.168.10.2
<b>B</b>	192.168.10.33

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

- 1 Click **Network Setting > Route > Static Route**.
- 2 Click **Add** to create a new route.



- 3 Configure the **Edit Static Route** screen using the following settings:
  - 3a Enter **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.
  - 3b Enter **192.168.1.253** (**R**'s IP address on N1) in the **IP Address** field under **Next Hop**.

**Edit Static Route**

Destination IP:

Subnet Mask:

Next Hop:

Interface:

IP Address:

Metric (1-255):

- 3a Click **Save**.

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



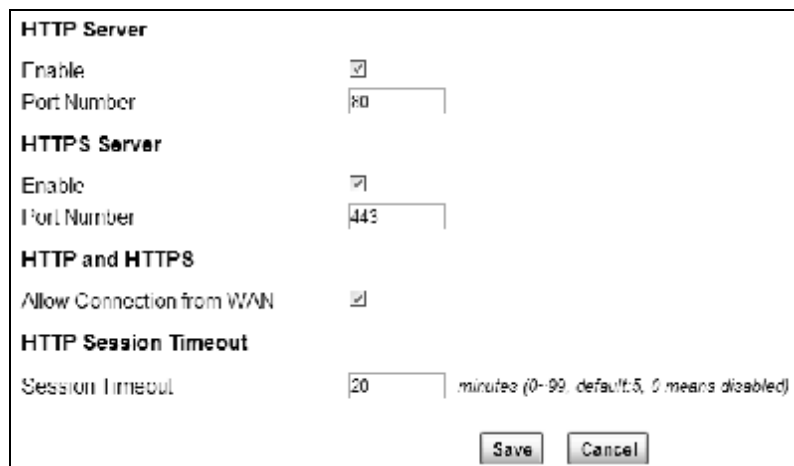
## 4.10 Remotely Managing Your MAX208M2W Series

The remote management feature allows you to log into the device through the Internet.

**Goal:** Set up the MAX208M2W Series to allow management requests from the WAN (Internet).

**See Also:** [Section 12.3 on page 169](#).

- 1 Open the **Maintenance > Remote MGMT > HTTP** screen.



**HTTP Server**  
Enable   
Port Number

**HTTPS Server**  
Enable   
Port Number

**HTTP and HTTPS**  
Allow Connection from WAN

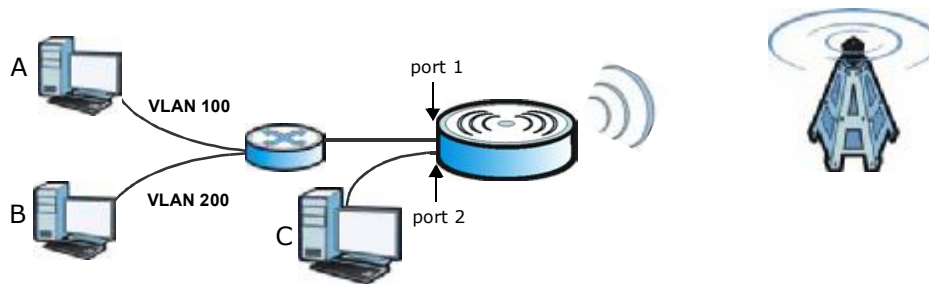
**HTTP Session Timeout**  
Session Timeout  minutes (0-99, default:5, 0 means disabled)

- 2 Select **Enable** in both **HTTP Server** and **HTTPS Server** sections and leave the **Port Number** settings as "80" and "443".
- 3 Select **Allow Connection from WAN**. This allows remote management connections not only from the local network but also the WAN network (Internet).
- 4 Click **Save**.

## 4.11 VLAN Configuration Example

This example assumes that you want port 1 to recognize VLAN 100 and VLAN 200 traffic sent from/to computers **A** and **B**. Port 2 is dedicated for transmitting and receiving VLAN-untagged and management traffic.

**Figure 17** VLAN Configuration Example



- 1 Connect your computer (**C** in the example) to the MAX208M2W Series's LAN port 2 and access the Web Configurator.
- 2 Log into the MAX208M2W Series.

- 3 Click **Network Setting** > **VLAN** and then click the PVID Group for port 2.

**Management VLAN**

VLAN ID: 0  
Priority: 0

Port Express Tagging

#	Tag
1	untagged
2	untagged

Total Num: 2

**Port Settings**

PVID Group

#	PVID Group	Priority
1	1	0
2	1	0

Total Num: 2

**VLAN Rules**

#	VID	Port 1		Port 2	
		Join	Tag	Join	Tag
1	1	Y	untagged	Y	untagged
2	2	Y	untagged	Y	untagged
3	3	Y	untagged	Y	untagged
4	4	Y	untagged	Y	untagged
5	5	Y	untagged	Y	untagged
6	6	Y	untagged	Y	untagged
7	7	Y	untagged	Y	untagged

Total Num: 7

Save Cancel

- 4 Select **MGMT** from the drop-down list, click **OK** in the section, and then click **Save** at the bottom of the screen.

**Port Settings**

PVID Group

#	PVID Group	Priority
1	1	0
2	1	0

Total Num: 2

**VLAN Rules**

#	VID	Port 1		Port 2	
		Join	Tag	Join	Tag
1	1	Y	untagged	Y	untagged
2	2	Y	untagged	Y	untagged
3	3	Y	untagged	Y	untagged
4	4	Y	untagged	Y	untagged
5	5	Y	untagged	Y	untagged
6	6	Y	untagged	Y	untagged
7	7	Y	untagged	Y	untagged

Total Num: 7

Save Cancel

- Click **Network Setting > WAN**. Change the MAX208M2W Series to bridge mode and then click **Save**.

Operation Mode: Bridge

WAN Protocol: Ethernet

Bridging LAN ARP: No

Get IP Method: From ISP

WAN IP Request Timeout: 120 seconds (0-820, default 120, unit: s)

WAN IP Address: 0.0.0.0

WAN IP Subnet Mask: 0.0.0.0

Gateway IP Address: 0.0.0.0

MTU: 1460

Clone MAC Address: 92:0C:EA:0B:01:01

**WAN DNS**

First DNS Server: From ISP 0.0.0.0

Second DNS Server: From ISP 0.0.0.0

Third DNS Server: From ISP 0.0.0.0

Save Cancel

- The MAX208M2W Series will restart. Wait until it completely restarts.
- Configure the IP address of your computer to be in the same network as the MAX208M2W Series's LAN. The default is 192.168.1.x where x can be 2 to 254.
- Open a browser and type the MAX208M2W Series's LAN IP address (for example, 192.168.1.1).
- Log into the MAX208M2W Series and then click **Network Setting > VLAN**.
- Enable VLAN and create VLAN 100 by entering VLAN 100 and the priority (7 in this example) in the **Management VLAN** section. The MAX208M2W Series requires to reboot again.

**Management VLAN**

VLAN ID: 0

Priority: 0

Port Egress Tagging

#	Tag
1	untagged
2	untagged
Total	

- After it completely restarts, log into the MAX208M2W Series. Click **Network Setting > VLAN**.

- 12 Since by default port 1 is associated with VLAN rule 1. Click the **VID** field to configure the settings as shown next. Click **OK** and then **Save**.

**Port Settings**

10 per page 1 page

#	PVID Group	Priority
1	1	0
2	MCMT	0

Total Num: 2

**VLAN Rules**

10 per page 1 page

#	VID	Port 1		Port 2	
		Join	Tag	Join	Tag
1	100	Y	tagged	N	untagged
2	2	Y	untagged	Y	untagged
3	3	Y	untagged	Y	untagged
4	4	Y	untagged	Y	untagged
5	5	Y	untagged	Y	untagged
6	6	Y	untagged	Y	untagged
7	7	Y	untagged	Y	untagged

Total Num: 7

Finally, you complete the settings. See [Section 7.19 on page 122](#) if you need more information about VLAN.



---

# **PART II**

## **Technical Reference**

---





# 5

## System Status

### 5.1 Overview

Use this screen to view a summary of your MAX208M2W Series connection status.

### 5.2 System Status

This screen allows you to view the current status of the device, system resources, and interfaces (LAN and WAN).

Click **System Status** to open this screen as shown next.

**Figure 18** System Status



The following tables describe the labels in this screen.

**Table 12** Status

LABEL	DESCRIPTION
System Information	
System Model Name	This field displays the MAX208M2W Series system model name. It is used for identification.
Software Version	This field displays the Web Configurator version number.
Firmware Version	This field displays the current version of the firmware inside the device.
Firmware Build Time	This field shows the date the firmware version was created.
Time	This field displays the current system time.
Uptime	This field displays how long the MAX208M2W Series has been running since it last started up.
System Resources	
Memory	This field displays what percentage of the MAX208M2W Series's memory is currently used. The higher the memory usage, the more likely the MAX208M2W Series is to slow down. Some memory is required just to start the MAX208M2W Series and to run the web configurator. You can reduce the memory usage by disabling some services; by reducing the amount of memory allocated to NAT and firewall rules (you may have to reduce the number of NAT rules or firewall rules to do so); or by deleting rules in functions such as incoming call policies, speed dial entries, and static routes.
CPU	This field displays what percentage of the MAX208M2W Series's CPU is currently used. The higher the CPU usage, the more likely the MAX208M2W Series is to slow down.
WiMAX	
Device Status	<p>This field displays the MAX208M2W Series current status for connecting to the selected base station.</p> <p><b>Scanning</b> - The MAX208M2W Series is scanning for available base stations.</p> <p><b>Ready</b> - The MAX208M2W Series has finished a scanning and you can connect to a base station.</p> <p><b>Connecting</b> - The MAX208M2W Series attempts to connect to the selected base station.</p> <p><b>Connected</b> - The MAX208M2W Series has successfully connected to the selected base station.</p>

**Table 12** Status (continued)

LABEL	DESCRIPTION
Connection Status	This field displays the status of the WiMAX connection between the MAX208M2W Series and the base station.  <b>Network Search</b> - The MAX208M2W Series is scanning for any available WiMAX connections.  <b>Disconnected</b> - No WiMAX connection is available.  <b>Network Entry</b> - A WiMAX connection is initializing.  <b>Normal</b> - The WiMAX connection has successfully established.
BSID	This field displays the MAC address of the base station to which the device is connected.
Frequency	This field indicates the frequency the MAX208M2W Series is using.
Signal Strength	This field indicates the strength of the connection that the MAX208M2W Series has with the base station.
Link Quality	This field indicates the relative quality of the link the MAX208M2W Series has with the base station.
WAN	
Status	This field indicates the status of the WAN connection to the MAX208M2W Series.
MAC Address	This field indicates the MAC address of the port making the WAN connection on the MAX208M2W Series.
IP Address	This field indicates the current IP address of the MAX208M2W Series in the WAN.
Subnet Mask	This field indicates the current subnet mask on the WAN.
Gateway	This field indicates the IP address of the gateway to which the MAX208M2W Series is connected.
MTU	This field indicates the Maximum Transmission Unit (MTU) between the MAX208M2W Series and the ISP servers to which it is connected.
DNS	This field indicates the Domain Name Server (DNS) to which your MAX208M2W Series is connected.
LAN	
MAC Address	This field indicates the MAC address of the port making the LAN connection on the MAX208M2W Series.
IP Address	This field displays the current IP address of the MAX208M2W Series in the LAN.
Subnet Mask	This field displays the current subnet mask in the LAN.
MTU	This field indicates the Maximum Transmission Unit (MTU) between the MAX208M2W Series and the client devices to which it is connected.
VOIP Phone	
Account1 Subscriber	This field displays the SIP number for SIP account 1.
Registered Status	This field displays whether SIP account 1 is already registered with a SIP server ( <b>Registered</b> or <b>Unregistered</b> ).
Account2 Subscriber	This field displays the SIP number for SIP account 2.

**Table 12** Status (continued)

LABEL	DESCRIPTION
Registered Status	This field displays whether SIP account 2 is already registered with a SIP server ( <b>Registered</b> or <b>Unregistered</b> ).
Line1 Status	This field displays whether phone line 1 (mapping to the <b>VoIP1</b> port) is in use or not (idle).
Line 2 Status	This field displays whether phone line 2 (mapping to the <b>VoIP2</b> port) is in use or not (idle).

## 6.1 Overview

This chapter shows you how to set up and manage the connection between the MAX208M2W Series and your ISP's base stations.

### 6.1.1 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 19** 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 20** 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.

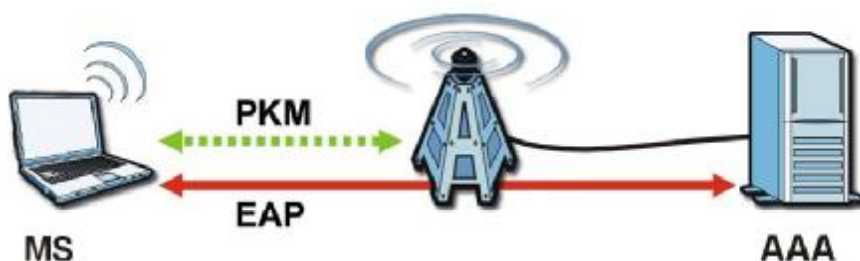
The radio frequency and bandwidth of the link between the MAX208M2W Series and the base station are controlled by the base station. The MAX208M2W Series follows the base station's configuration.

### 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 21** Using an AAA Server

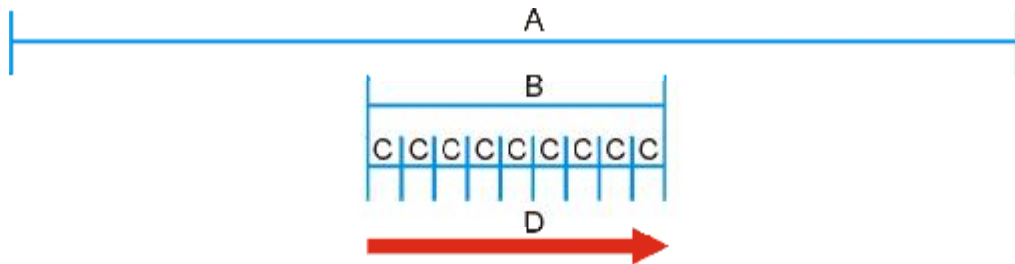


In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

## Frequency Ranges

The following figure shows the MAX208M2W Series searching a range of frequencies to find a connection to a base station.

**Figure 22** Frequency Ranges



In this figure, **A** is the WiMAX frequency range. “WiMAX frequency range” refers to the entire range of frequencies the MAX208M2W Series 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 MAX208M2W Series searching for a connection.

Have the MAX208M2W Series 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 MAX208M2W Series 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.

## Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the MAX208M2W Series to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

## Certificate File Formats

The certification authority 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. The MAX208M2W Series currently allows the importation of a PKCS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

## CINR

Carrier to Interference-plus-Noise Ratio (CINR) measures the effectiveness of a wireless signal and plays an important role in allowing the MAX208M2W Series to decode signal bursts. If a burst has a high signal strength and a high interference-plus-noise ratio, it can use Digital Signal Processing (DSP) to decode it; if the signal strength is lower, it can switch to an alternate burst profile.

## RSSI

Received Signal Strength Indicator (RSSI) measures the relative strength of a given wireless signal. This is important in determining if a signal is below the Clear-To-Send (CTS) threshold. If it is below the arbitrarily specified threshold, then MAX208M2W Series is free to transmit any data packets.

## EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The MAX208M2W Series supports EAP-TLS and EAP-TTLS (at the time of writing, TTLS is not available in Windows Vista). For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). Certificates (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.



## 6.2 Connection Settings

This screen allows you to configure how the MAX208M2W Series connects to the base stations on the WiMAX network.

Click **WiMAX > Profile > Connection Settings** to open this screen as shown next.

**Figure 23** Connection Settings Screen

This screen contains the following fields:

**Table 13** Connection Settings

LABEL	DESCRIPTION
Connection Option Settings	
Auto Reconnect	Select the interval in seconds that the MAX208M2W Series waits after getting disconnected from the base station before attempting to reconnect.
Auto Connect Mode	Select the auto connect mode. <ul style="list-style-type: none"> <li>• <b>By channel power</b> - Auto connects to the base station if the signal strength of the channel is sufficient for the MAX208M2W Series.</li> <li>• <b>By CINR</b> - Auto connects to the base station if the signal-to-noise ratio is sufficient for the MAX208M2W Series.</li> </ul>
Enable Handover	Select this to maintain connectivity while the MAX208M2W Series switches its connection from one base station to another base station.
Enable Idle Mode	Select this to have the MAX208M2W Series 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.

**Table 13** Connection Settings (continued)

LABEL	DESCRIPTION
Idle Mode Interval	Set the idle duration in minutes. This is how long the MAX208M2W Series waits during periods of no activity before going into idle mode.
CINR & RSSI Refresh Interval	Set the refresh interval in milliseconds for calculating the signal-to-noise measurement (CINR) and signal strength measurement (RSSI) of the MAX208M2W Series.
LDRP (Low Data Rate Protection)	Enter the Low Data Rate Protection (LDRP) time in milliseconds. If the uplink/downlink data rate is smaller than the LDRP time, the MAX208M2W Series sends a disconnect request to the base station.
LDRP TX Rate	Enter the outgoing data rates for LDRP in bytes per second.
LDRP RX Rate	Enter the incoming data rates for LDRP in bytes per second.
Connection Type Settings	
Mode Select	Select how the MAX208M2W Series connects to the base station. <ul style="list-style-type: none"> <li>• <b>Auto Connect Mode</b> - The device connects automatically to the first base station in range.</li> <li>• <b>Network Search Mode</b> - The device scans for available base stations then connects to the best one it can.</li> </ul>
BSID	This displays the MAC address of a base station within range of the MAX208M2W Series.
Preamble ID	The preamble ID is the index identifier in the header of the base station's broadcast messages. In the beginning of a mobile stations' network entry process, it searches for the preamble and uses it to additional channel information.  The preamble ID is used to synchronize the upstream and downstream transmission timing with the base station.
Frequency (MHz)	This field displays the radio frequency of the MAX208M2W Series's connection to the base station.
Bandwidth (MHz)	This field displays the bandwidth of the base station in megahertz (MHz).
RSSI (dBm)	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR (dB) R3/R1	This field displays the average Carrier to Interference plus Noise Ratio for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Search	Click this to have the MAX208M2W Series scan for base stations.

## 6.3 Frequency Settings

Use this screen to have the WiMAX Device to scan one or more specific radio frequencies (given by your WiMAX service provider) to find available connections to base stations.

Click **WiMAX > Profile > Frequency Settings** to open this screen as shown next.

**Figure 24** Frequency Settings Screen (By List)

Setting Type:

Join Wide Scan Result:

Default Bandwidth:  MHz

**A**

#	Frequency(KHz)	Bandwidth(MHz)
1	3550000	10

Total Num: 1

Valid Band Info:

**B**

#	Band Start(KHz)	Band End(KHz)
1	3300000	3600000

Total Num: 1

**Figure 25** Frequency Settings Screen (By Range)

Setting Type:

**A**

#	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)
1				0

Total Num: 1

Valid Band Info:

**B**

#	Band Start(KHz)	Band End(KHz)
1	3300000	3600000

Total Num: 1

This screen contains the following fields:

**Table 14** Frequency Settings

LABEL	DESCRIPTION
Setting Type	<p>Select whether to scan base stations by entering specific frequency(-ies) (<b>By List</b>) or a range of frequencies (<b>By Range</b>).</p> <p>Note: When you select <b>By Range</b>, you can only configure one range of frequencies in this screen. To configure multiple frequency ranges, use the <b>WiMAX &gt; Wide Scan</b> screen.</p> <p>Note: Some settings in this screen are only available depending on the <b>Setting Type</b> selected.</p>
Join Wide Scan Result	<p>The scanning result of the frequency to scan you configured in this screen will be shown in the <b>WiMAX &gt; Connect</b> screen. Select this option to determine whether to also append the wide scanning result (configured in the <b>WiMAX &gt; Wide Scan</b> screen) to the same table.</p>
Default Bandwidth	<p>Select the default bandwidth (size) per frequency band you specify in table <b>A</b>.</p>
<b>A</b> (When <b>By List</b> is selected in the <b>Setting Type</b> field)	
Frequency (KHz)	<p>This displays the center frequency of an frequency band in kilohertz (KHz).</p> <p>Click the number to modify it.</p> <p>Enter the center frequency in this field when you are adding an entry.</p>
Bandwidth (MHz)	<p>This displays the bandwidth of the frequency band in megahertz (MHz). If you set a center frequency to 3400000 KHz with the bandwidth of 10 MHz, then the frequency band is from 3399500 to 3400500 KHz.</p> <p>Click the number to modify it.</p> <p>Enter the bandwidth of the frequency band in this field when you are adding an entry.</p>
Delete	<p>Click this button to remove an item from the list.</p>
Add	<p>Click this button to add an item to the list.</p>
OK	<p>Click this button to save any changes made to the list.</p>
<b>A</b> (When <b>By Range</b> is selected in the <b>Setting Type</b> field)	
Start Frequency (KHz)	<p>This indicates the beginning of a frequency band in kilohertz (KHz).</p> <p>Click this field to modify it.</p> <p>Enter the beginning frequency when you are adding an entry.</p>
End Frequency (KHz)	<p>This indicates the end of the frequency band in kilohertz (KHz).</p> <p>Click this field to modify it.</p>
Step (KHz)	<p>This indicates the frequency step within each band in kilohertz (KHz).</p> <p>Click this field to modify it.</p>
Bandwidth (MHz)	<p>This indicates the bandwidth in megahertz (MHz).</p> <p>Click this field to modify it.</p>

**Table 14** Frequency Settings (continued)

LABEL	DESCRIPTION
OK	Click this button to save any changes made to the list.
Valid Band Info ( <b>B</b> )  This table displays the entire frequency band the MAX208M2W Series supports. The frequenc(ies) to scan that you configured in table <b>A</b> must be within this range.	
Band Start (KHz)	This indicates the beginning of the frequency band in kilohertz (KHz).
Band End (KHz)	This indicates the end of the frequency band in kilohertz (KHz).

## 6.4 Authentication Settings

These settings allow the WiMAX Device to establish a secure (authenticated) connection with the service provider.

Click **WiMAX > Profile > Authentication Settings** to open this screen as shown next.

**Figure 26** Authentication Settings Screen

Authentication Mode	User authentication	▼
Data Encryption		
AES-CCM	<input checked="" type="checkbox"/>	
AES-CBC	<input checked="" type="checkbox"/>	
Key Encryption		
AES-key wrap	<input checked="" type="checkbox"/>	
AES-ECB	<input checked="" type="checkbox"/>	
<b>EAP Supplicant</b>		
EAP Mode	EAP-TLS	▼
Anonymous ID	<input type="text"/>	
Server Root CA Cert. File	<input type="text"/>	Browse...
Server Root CA Cert. Info	No certificate file found	▲▼
Device Cert. File	<input type="text"/>	Browse...
Device Cert. Info	No certificate file found	▲▼
Device Private Key	<input type="text"/>	Browse...
Device Private Key Info	No private key found	▲▼
Device Private Key Password	<input type="password"/>	
Inner Mode	MS-CHAPv2	▼
Username	<input type="text"/>	
Password	<input type="password"/>	
<b>Options</b>		
Enable Auth Mode Decoration in EAP Outer ID	<input type="checkbox"/>	
Enable Service Mode Decoration in EAP Outer ID	<input type="checkbox"/>	
Random Outer ID	<input type="checkbox"/>	
Ignore Cert Verification	<input checked="" type="checkbox"/>	
Same EAP OuterID in ReAuth	<input type="checkbox"/>	
MAC address in EAP-TLS outer ID	<input type="checkbox"/>	
Delete existed Root Certificate file	<input type="checkbox"/>	
Delete existed Device Certificate file	<input type="checkbox"/>	
Delete existed Private Key	<input type="checkbox"/>	

This screen contains the following fields:

**Table 15** Authentication Settings

LABEL	DESCRIPTION
Authentication Mode	Select the authentication mode from the list.  The MAX208M2W Series supports the following authentication modes: <ul style="list-style-type: none"> <li>• No authentication</li> <li>• User authentication</li> <li>• Device authentication</li> <li>• User and device authentication</li> </ul>
Data Encryption	
AES-CCM	Select this to enable AES-CCM encryption. CCM combines counter-mode encryption with CBC-MAC authentication.
AES-CBC	Select this to enable AES-CBC encryption. CBC creates message authentication code from a block cipher.
Key Encryption	
AES-key wrap	Select this to encapsulate cryptographic keys in a symmetric encryption algorithm.
AES-ECB	Select this to divide cryptographic keys into blocks and encrypt them separately.
EAP Supplicant	
EAP Mode	Select an Extensible Authentication Protocol (EAP) mode.  The MAX208M2W Series supports the following: <ul style="list-style-type: none"> <li>• <b>EAP-TLS</b> - In this protocol, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.</li> <li>• <b>EAP-TTLS</b> - This protocol is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.</li> </ul>
Anonymous ID	Enter the anonymous ID used for EAP supplicant authentication.
Server Root CA Cert File	Browse for and choose a server root certificate file, if required.
Server Root CA Info	This field displays information about the assigned server root certificate.
Device Cert File	Browse for and choose a device certificate file, if required.
Device Cert Info	This field displays information about the assigned device certificate.

**Table 15** Authentication Settings (continued)

LABEL	DESCRIPTION
Device Private Key	Browse for and choose a device private key, if required.
Device Private Key Info	This field displays information about the assigned device private key.
Device Private Key Password	Enter the device private key, if required.
Inner Mode	<p>Sets the EAP-TTLS inner mode.</p> <p>The MAX208M2W Series supports the following:</p> <ul style="list-style-type: none"> <li>• <b>MS-CHAP v2</b> - This is version 2 of Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.</li> <li>• <b>MS-CHAP</b> - This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.</li> <li>• <b>CHAP</b> - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification.</li> <li>• <b>MD5</b> - Message-Digest, algorithm 5, (MD5) encryption is typically used for checking file integrity. Because this encryption protocol contains a number of serious security flaws it is generally not recommended that you use it for authentication security.</li> <li>• <b>PAP</b> - Password Authentication Protocol uses unencrypted plaintext to send a passwords for authentication over the network. It's probably not a good idea to rely on this for security.</li> </ul>
Username	Enter the username required for the EAP-TTLS inner method.
Password	Enter the password required for the EAP-TTLS inner method.
Options	
Enable Auth Mode Decoration in EAP Outer ID	Select this to enable authentication mode.
Enable Service Mode Decoration in EAP Outer ID	Select this to enable service mode.
Random Outer ID	Select this to allow the MAX208M2W Series to generate a 16-byte random number as a username for the EAP Identity Response message.
Ignore Cert Verification	Select this to ignore base station certification verification when a certificate is received during EAP-TLS or EAP-TTLS.
Same EAP OuterID in ReAuth	Select this to use the same EAP to the outer ID when reauthenticating.
MAC address in EAP-TLS outer Id	Adds the MAC address of the MAX208M2W Series to the outer ID while the EAP mode is set to EAP-TLS.



**Table 15** Authentication Settings (continued)

LABEL	DESCRIPTION
Delete existed Root Certificate file	Select this to delete an existing root certificate file from the MAX208M2W Series.
Delete existed Device Certificate file	Select this to delete an existing device certificate file from the MAX208M2W Series.
Delete existed Private Key	Select this to delete an existing private key from the MAX208M2W Series.

## 6.5 Connect

This screen allows you to view the available WiMAX frequency band(s) and base station(s) the MAX208M2W Series found through scanning and choose a base station to which to connect.

Click **WiMAX > Connect** to open this screen as shown next.

**Figure 27** Connect Screen

Applied Frequency Information						
#	Frequency(KHz)	Bandwidth(MHz)				
1	3550000	10				
Total Num: 1						
Available Network List						
				Auto Connect Mode	Connect	Disconnect
#	BSID	Preamble ID	Frequency (MHz)	Bandwidth (MHz)	RSSI (dBm)	CINR (dB) R3/R1
1	F7:48:0A:01:13:21	42	3550	10	-78.82	18.95/14.59
Total Num: 1						Search
Connected BS Info						
#	Device Status	UMAC State	BSID	Frequency(MHz)	RSSI(dBm)	CINR(dB)
1	Ready	Disconnected	00:00:00:00:00	0	0.00	0.00
Total Num: 1						

This screen contains the following fields:

**Table 16** Connect

LABEL	DESCRIPTION
Applied Frequency Information	
This table shows the scanning result you made in the <b>WiMAX &gt; Profile &gt; Frequency Settings</b> and <b>WiMAX &gt; Wide Scan</b> screens.	
Note: You cannot see the wide scanning result that you made in <b>WiMAX &gt; Wide Scan</b> screen if the <b>Join Wide Scan Result</b> is set to <b>No</b> in the <b>WiMAX &gt; Profile &gt; Frequency Settings</b> screen.	
Frequency (KHz)	This field displays the available center frequency of a frequency band in kilohertz (KHz).
Bandwidth (MHz)	This field displays the bandwidth of the frequency band in megahertz (MHz).
Available Network List	
Connected Mode	Select a connect mode: <ul style="list-style-type: none"> <li>• <b>Auto Connect Mode</b> - This allows the MAX208M2W Series to connect to any of the base stations on the list automatically.</li> <li>• <b>Network Search Mode</b> - This allows the MAX208M2W Series to connect to a user-specified base station. Select this option, choose a base station, click <b>Connect</b>.</li> </ul>
Connect	Click this to connect to the selected base station.
Disconnect	Click this to disconnect from the selected base station.
BSID	This field displays the base station MAC address.
Preamble ID	This field displays the preamble ID.  The preamble ID is the index identifier in the header of the base station's broadcast messages. In the beginning of a mobile stations's network entry process, it searches for the preamble and uses it to additional channel information.  The preamble ID is used to synchronize the upstream and downstream transmission timing with the base station.
Frequency (MHz)	This field displays the center frequency the base station uses in kilohertz (KHz).
Bandwidth (MHz)	This field displays the frequency band bandwidth the base station uses in megahertz (MHz).
RSSI (dBm)	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR (dB) R3/R1	This field displays the average Carrier to Interference plus Noise Ratio for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Search	Click this to have the MAX208M2W Series scan for base stations in the frequency band(s) listed in the <b>Applied Frequency Information</b> table.
Connected BS Info	

**Table 16** Connect (continued)

LABEL	DESCRIPTION
Device Status	<p>This field displays the MAX208M2W Series current status for connecting to the selected base station.</p> <p><b>Scanning</b> - The MAX208M2W Series is scanning for available base stations.</p> <p><b>Ready</b> - The MAX208M2W Series has finished scanning and you can connect to a base station.</p> <p><b>Connecting</b> - The MAX208M2W Series attempts to connect to the selected base station.</p> <p><b>Connected</b> - The MAX208M2W Series has successfully connected to the selected base station.</p>
UMAC State	<p>This field displays the status of the WiMAX connection between the MAX208M2W Series and the base station.</p> <p><b>Network Search</b> - The MAX208M2W Series is scanning for any available WiMAX connections.</p> <p><b>Disconnected</b> - No WiMAX connection is available.</p> <p><b>Network Entry</b> - A WiMAX connection is initializing.</p> <p><b>Normal</b> - The WiMAX connection has been successfully established.</p>
BSID	<p>This field displays the MAC address of the base station to which the MAX208M2W Series is connected.</p>
Frequency (MHz)	<p>This field displays the frequency the base station uses in megahertz (MHz).</p>
RSSI (dBm)	<p>This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.</p>
CINR (dB)	<p>This field displays the average Carrier to Interference plus Noise Ratio for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.</p>

## 6.6 Wide Scan

This screen allows you to discover base stations by entering one or more frequency ranges and bandwidth on which to scan.

Click **WiMAX > Wide Scan** to open this screen as shown next.

**Figure 28** Wide Scan Screen

**Wide Scan Settings**

Auto Wide Scan

Wide Scan Range

#	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)	
1	3500000	3600000	250	10	<input type="button" value="🗑️"/>

Total Num: 1

**Wide Scan Result**

#	Frequency (KHz)	Bandwidth (MHz)
1	3550000	10
2	3570000	10

Total Num: 2

This screen contains the following fields:

**Table 17** Wide Scan

LABEL	DESCRIPTION
Wide Scan Settings	
Auto Wide Scan	Use this to enable ( <b>Yes</b> ) or disable ( <b>No</b> ) automatically scanning for base stations.
Wide Scan Range	
Start Frequency (KHz)	Enter the start frequency in kilohertz (KHz) for a wide scan range.
End Frequency (KHz)	Enter the end frequency in kilohertz (KHz) for a wide scan range.
Step (KHz)	Enter the step increment in kilohertz (KHz) that the wide scan jumps each time it scans between the start and end frequencies.
Bandwidth (MHz)	Enter the frequency bandwidth to be scanned.
Delete	Click this to remove a range of frequencies from the wide scan range list.
Add	Click this to add a range of frequencies to the wide scan range list.
OK	Click this so save any changes to the wide scan range list.
Wide Scan Result	
This table displays the available frequency band(s) found through the wide scan.	

**Table 17** Wide Scan (continued)

LABEL	DESCRIPTION
Frequency (KHz)	This field displays the frequency in kilohertz (KHz).
Bandwidth (MHz)	This field displays the bandwidth in megahertz (MHz).
Search	Click this to initiate a wide scan.
Clear	Click this to clear the wide scan results.

## 6.7 Link Status

This screen provides a general overview of the current WiMAX connection with the service provider.

Click **WiMAX > Link Status** to open this screen as shown next.

**Figure 29** Link Status Screen

Connection Status	
Profile	Wimax
BSID	00:00:00:00:00:00
RSSI	-0.01 dBm
CINR R3	-0.01 dB
CINR R1	-0.01 dB
CINR Std Dev	-0.01 dB
Frequency	0 KHz
TX Power	0 dBm
UL MCS	QPSK [CC] 1/2
DL MCS	QPSK [CC] 1/2
RF Temperature	24 C
Handover Success	0
Handover Fail	0

This screen contains the following fields:

**Table 18** Link Status

LABEL	DESCRIPTION
Profile	This field displays the profile name.
BSID	This field displays the MAC address of the base station to which the MAX208M2W Series is currently connected.
RSSI	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR R3	This field displays the average Carrier to Interference plus Noise Ratio (R3) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.

**Table 18** Link Status (continued)

LABEL	DESCRIPTION
CINR R1	This field displays the average Carrier to Interference plus Noise Ratio (R1) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
CINR Std Dev	This field displays the average Carrier to Interference plus Noise Ratio (Std Dev) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Frequency	This field displays the frequency in kilohertz (KHz).
TX Power	This field displays the transmission power of the MAX208M2W Series in dBm.
UL MCS	This field displays the Uplink Modulation and Coding Sequence (UL MCS).
DL MCS	This field displays the Downlink Modulation and Coding Sequence (DL MCS).
RF Temperature	This field displays the temperature in centigrade of the MAX208M2W Series's RF circuit.
Handover Success	This field displays how many times the MAX208M2W Series had ever successfully switched its connection from one base station to another base station, since the MAX208M2W Series last restarted.
Handover Fail	This field displays how many times the MAX208M2W Series had been failed to switch its connection from one base station to another base station, since the MAX208M2W Series last restarted.

## 6.8 Link Statistics

This screen provides a detailed overview of the current WiMAX connection with the service provider..

Click **WiMAX > Link Statistics** to open this screen as shown next.

**Figure 30** Link Statistics Screen

Link			
TX Connections		Downlink PDU	undefined
RX Connections	undefined	Downlink SDU	undefined
Frame Number	undefined	DL Discard Frame	undefined
Frame Duration	undefined	UL Fragmentation	undefined
Init Rang. Code Start	undefined	DL Unpacking	undefined
Init Rang. Code End	undefined	DL Defrag	undefined
Periodic Rang. Code Start	undefined	Mng Msg Send	undefined
Periodic Rang. Code End	undefined	Mng Msg Recv	undefined
Uplink PDU	undefined	Mng Msg Drop	undefined
Uplink SDU	undefined	DL frequency	undefined
PSD Ratio	undefined %		
HARQ			
TX Burst	undefined	Re-TX Burst	undefined
RX Valid Burst	undefined	Rx Invalid Burst	undefined
RX Dup. Burst	undefined	Uplink Retrans. Ratio	undefined %
Downlink NAK Ratio	undefined %		
TX/RX			
Packets Sent	0	Packets Received	0
Transmit Bytes	0	Received Bytes	0
Transmit Bytes Rate	0	Received Bytes Rate	0
MCS			
QPSK-1/2		QPSK-3/4	undefined
16QAM-1/2	undefined	16QAM-3/4	undefined
64QAM-1/2	undefined	64QAM-2/3	undefined
64QAM-3/4	undefined	64QAM-5/6	undefined

This screen contains the following sections:

**Table 19** Link Statistics

LABEL	DESCRIPTION
Link	This section provides a detailed overview of link statistics.
HARQ	This section provides a detailed overview of Hybrid Automatic Repeat Request link statistics.
TX/RX	This section provides a detailed overview of transmission and receiving link statistics.
MCS	This section provides a detailed overview of Modulation and Coding Sequence (MCS) link statistics

## 6.9 Connection Info

This screen displays all of the connections made through the WiMAX device since its last reboot.

Click **WiMAX > Connection Info** to open this screen as shown next.

**Figure 31** Connection Info Screen

#	Active Connection CID	Connection Type
Total Num: 0		

This screen contains the following fields:

**Table 20** Connection Info

LABEL	DESCRIPTION
Active Connection CID	This displays the unique, unidirectional 16-bit Connection Identifier (CID) for an active connection.
Connection Type	This displays the type of connection.

## 6.10 Service Flow

This screen displays data priority information for all of the connections made through the WiMAX device since its last reboot.

Click **WiMAX > Service Flow** to open this screen as shown next.

**Figure 32** Service Flow Screen

#	SFID	SF Status	SF Direction
Total Num: 0			

This screen contains the following fields:

**Table 21** Service Flow

LABEL	DESCRIPTION
SFID	This displays a 32-bit service flow identifier.
SF Status	This display the service flow status.
SF Direction	This displays the service flow direction.



# 7

## Network Setting

### 7.1 Overview

This chapter shows you how to configure the MAX208M2W Series's network setting.

#### 7.1.1 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.

##### **DHCP**

A DHCP (Dynamic Host Configuration Protocol) server can assign your MAX208M2W Series an IP address, subnet mask, DNS and other routing information when it's turned on.

## 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; 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 MAX208M2W Series supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields are not specified, for instance, left as 0.0.0.0, the MAX208M2W Series tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the MAX208M2W Series, the MAX208M2W Series 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. This way, the MAX208M2W Series can pass the DNS servers to the computers and the computers can query the DNS server directly without the MAX208M2W Series's intervention.

## 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:

- **RX/TX** - the MAX208M2W Series will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **RX Only** - the MAX208M2W Series will not send any RIP packets but will accept all RIP packets received.
- **TX Only** - the MAX208M2W Series will send out RIP packets but will not accept any RIP packets received.
- **None** - the MAX208M2W Series 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 MAX208M2W Series 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.

### Port Forwarding

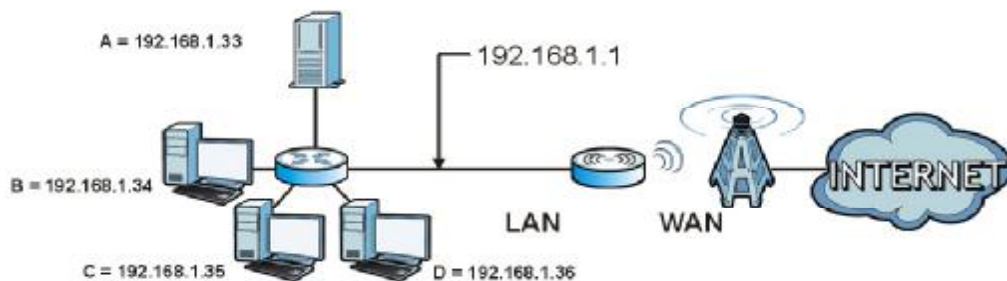
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

With port forwarding, you can 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



## Trigger Ports

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The MAX208M2W Series records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the MAX208M2W Series's WAN port receives a response with a specific port number and protocol ("incoming" port), the MAX208M2W Series forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

## ALG

Some applications, such as SIP, cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. Some NAT routers may include a SIP Application Layer Gateway (ALG). An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer.

A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream.

## UPnP

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

### How do I know if I'm using UPnP?

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

### NAT Traversal

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

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

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

### Cautions with UPnP

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

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

### UPnP and ZyXEL

ZyXEL has received UPnP certification from the official UPnP Forum (<http://www.upnp.org>). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device).

The MAX208M2W Series only sends UPnP multicasts to the LAN.

### **Content Filter**

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain specific URL keywords.

## 7.2 WAN

Use these settings to configure the WAN connection between the WiMAX Device and the service provider.

Click **Network Setting > WAN** to open this screen as shown next.

**Figure 34** WAN Screen

Operation Mode	NAT	▼
WAN Protocol	Ethernet	▼
Bridging LAN ARP	No	▼
Get IP Method	From ISP	▼
WAN IP Request Timeout	120	seconds (0~600, default: 120, infinite:0)
WAN IP Address	0.0.0.0	
WAN IP Subnet Mask	0.0.0.0	
Gateway IP Address	0.0.0.0	
MTU	1500	
Clone MAC Address	00:0C:E7:0B:01:01	
<b>WAN DNS</b>		
First DNS Server	From ISP	▼ 0.0.0.0
Second DNS Server	From ISP	▼ 0.0.0.0
Third DNS Server	From ISP	▼ 0.0.0.0

This screen contains the following fields:

**Table 22** WAN

LABEL	DESCRIPTION
Operation Mode	Select the MAX208M2W Series's operational mode. <ul style="list-style-type: none"> <li>• <b>Bridge</b> - This puts the MAX208M2W Series in bridge mode, acting as a transparent middle man between devices on the LAN and the devices on the WAN.</li> <li>• <b>NAT</b> - This allows the MAX208M2W Series to tag frames for NAT, allowing devices on the LAN to use their own internal IP addresses while communicating with devices on the WAN.</li> </ul>
WAN Protocol	Select the protocol the MAX208M2W Series uses to connect to the WAN. <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Ethernet</b> - Select this if you have a persistent connection to the network.</li> <li>• <b>PPPoE</b> - Select this if must log into the network before initiating a persistent connection.</li> <li>• <b>GRE Tunnel</b> - Select this if you connect to the network using Point-to-Point Protocol to create VPNs.</li> <li>• <b>EtherIP</b> - Select this if you need to tunnel Ethernet and IEEE 802.3 MAC frames across an IP Internet.</li> </ul>
Bridging LAN ARP	This option enables or disables allow ARP requests to cross the MAX208M2W Series.
Get IP Method	Select how the MAX208M2W Series receives its IP address. <ul style="list-style-type: none"> <li>• <b>User</b> - Select this to manually enter the IP address the MAX208M2W Series uses.</li> <li>• <b>From ISP</b> - Select to automatically get the IP address the MAX208M2W Series uses from the ISP.</li> </ul>
WAN IP Request Timeout	Enter the number of seconds the MAX208M2W Series waits for an IP from the ISP before it times out.
WAN IP Address	If the MAX208M2W Series gets its IP from the user, enter the IP address it is to use.
WAN IP Subnet Mask	If the MAX208M2W Series gets its IP from the ISP, enter the IP address it is to use.
Gateway IP Address	If the MAX208M2W Series gets its gateway IP address from the user, enter the IP address it is to use.
MTU	Enter the Maximum Transmission Unit (MTU) for the MAX208M2W Series. This is the largest protocol unit that the MAX208M2W Series allows to pass through it.

**Table 22** WAN (continued)

LABEL	DESCRIPTION
Clone MAC Address	Enter a MAC address here for registering bridged devices on the network if their current MAC addresses are causing problems. For example, this can happen when a desktop computer swaps network interface cards; the original NIC may have used its MAC address to register itself on the network and now the new NIC is unrecognized. Using a MAC address that you know is valid, i.e. a "clone", allows that device to stay registered.
First~Third DNS Server	Select how the MAX208M2W Series acquires its DNS server address. <ul style="list-style-type: none"> <li>• <b>From ISP</b> - Select this to have the MAX208M2W Series acquire its DNS server address from the ISP.</li> <li>• <b>User Define</b> - Select this to manually enter the DNS server used by the MAX208M2W Series.</li> </ul>

## 7.3 PPPoE

Use these settings to configure the PPPoE connection between the WiMAX Device and the service provider.

Click Network Setting > WAN > PPPoE.

**Figure 35** PPPoE Screen

**PPPoE**

User Name

Password

Retype Password

Auth Protocol  PAP  CHAP  MSCHAPv1  MSCHAPv2

MPPE Encryption

MPPE Stateful

Idle Timeout  (0~86400 seconds; enter 0 to never timeout)

AC Name

DNS overwrite

Connection Trigger

Connection Timeout  (0~86400 seconds; enter 0 to never timeout)



This screen contains the following fields:

**Table 23** PPPoE

LABEL	DESCRIPTION
User Name	Enter the username for PPPoE login into the WAN network.
Password	Enter the password for PPPoE login into the WAN network.
Retype Password	Retype the password to confirm it.
Auth Protocol	Select a PPPoE authentication protocol. The MAX208M2W Series supports the following: <ul style="list-style-type: none"> <li>• <b>CHAP</b> - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification.</li> <li>• <b>PAP</b> - Password Authentication Protocol uses unencrypted plaintext to send a passwords for authentication over the network. It's probably not a good idea to rely on this for security.</li> <li>• <b>MS-CHAP v1/2</b> -This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.</li> </ul>
MPPE Encryption	Use this option to enable or disable authentication through Microsoft Point-To-Point Encryption (MPPE) protocol.through Microsoft Point-To-Point Encryption (MPPE) protocol.
MPPE Stateful	Use this option to allow or disallow the MAX208M2W Series to use the Microsoft Point-To-Point Encryption (MPPE) protocol for stateful peer negotiation.
Idle Timeout	Enter the number of second the MAX208M2W Series waits during authentication before timing out.
AC Name	Enter the access concentrator name for the PPPoE interface if your ISP uses an AC PPPoE service.
DNS Overwrite	Use this option to allow or disallow the MAX208M2W Series to overwrite DNS static DNS entries on client devices.
Connection Trigger	Set whether the MAX208M2W Series is persistently connected to the WAN ( <b>AlwaysOn</b> ) or you must click the PPPoE Connect button each time you want to get on the WAN ( <b>Manual</b> ).
Connection Timeout	Enter in seconds the duration the MAX208M2W Series waits for idle activity before disconnecting from the WAN.
PPPoE Connect	Click this to connect to the WAN using PPPoE.
PPPoE Disconnect	Click this to disconnect from the WAN.

## 7.4 GRE

Use these settings to configure the peer setting of the Generic Routing Encapsulation (GRE) tunnel between the WiMAX Device and another GRE peer.

Click **Network Setting > WAN > GRE** to open this screen as shown next.

**Figure 36** GRE Screen

This screen contains the following fields:

**Table 24** GRE

LABEL	DESCRIPTION
Peer IP Address	Enter the IP address of the GRE peer.

## 7.5 EtherIP

Use these settings to configure the peer setting of the EtherIP tunnel between the WiMAX Device and another EtherIP peer.

Click **Network Setting > WAN > EtherIP** to open this screen as shown next.

**Figure 37** EtherIP Screen

This screen contains the following fields:

**Table 25** EtherIP

LABEL	DESCRIPTION
Peer IP Address	Enter the IP address of the EtherIP peer.

## 7.6 IP

Use these settings to configure the LAN connection between the WiMAX Device and your local network.

Click **Network Setting > LAN > IP** to open this screen as shown next.

**Figure 38** IP Screen

IP Address	<input type="text" value="192.168.1.1"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>

This screen contains the following fields:

**Table 26** IP

LABEL	DESCRIPTION
IP address	Enter the IP address of the LAN interface for the MAX208M2W Series.
IP Subnet Mask	Enter the IP subnet masks of the LAN interface for the MAX208M2W Series.

## 7.7 DHCP

Use these settings to configure whether the WiMAX Device functions as a DHCP server for your local network, or a DHCP relay between the local network and the service provider. You can also disable the DHCP functions.

Click **Network Setting > LAN > DHCP** to open this screen as shown next.

**Figure 39** DHCP Screen

**DHCP Server**

DHCP Mode: Server

Start IP: 192.168.1.33

End IP: 192.168.1.132

Lease Time: 1440 (minutes)

Relay IP: 0.0.0.0

**DNS Server assigned by DHCP Server**

First DNS Server: From ISP 0.0.0.0

Second DNS Server: From ISP 0.0.0.0

Third DNS Server: From ISP 0.0.0.0

**Static DHCP**

10 per page

#	MAC Address	IP Address
Total Num: 0		

Add OK

**DHCP Leased Hosts**

10 per page

#	MAC Address	IP Address	Remaining Time
1	00:21:85:0C:44:1A	192.168.1.33	23:58:50
Total Num: 1			

Refresh

This screen contains the following fields:

**Table 27** DHCP

LABEL	DESCRIPTION
DHCP Server	
DHCP Mode	<p>Select this if you want the MAX208M2W Series to be the DHCP server on the LAN. As a DHCP server, the MAX208M2W Series assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information.</p> <ul style="list-style-type: none"> <li><b>None</b> - This disables DHCP mode for the MAX208M2W Series.</li> <li><b>Server</b> - This sets the MAX208M2W Series as a DHCP server for the LAN.</li> <li><b>Relay</b> - This sets the MAX208M2W Series as a DHCP relay for the LAN, allowing it to pass-through IP addresses assigned to LAN devices from the ISP servers.</li> </ul>

**Table 27** DHCP (continued)

LABEL	DESCRIPTION
Start IP	Enter the start IP address from which the MAX208M2W Series begins allocating IP addresses.
End IP	Enter the end IP address at which the MAX208M2W Series ceases allocating IP addresses.
Lease Time	Enter the duration in minutes that devices on the LAN retain their DHCP-issued IP addresses. At the end of the lease time, they poll the MAX208M2W Series for a renewed or replacement IP.
Relay IP	Enter the name of the IP address to be used.
DNS Server Assigned by the DHCP Server	
First~Third DNS Server	Select how the MAX208M2W Series acquires its DNS server address. <ul style="list-style-type: none"> <li>• <b>None</b> - Select this to not use a DNS server.</li> <li>• <b>From ISP</b> - Select this to have the MAX208M2W Series acquire its DNS server address from the ISP.</li> <li>• <b>User Define</b> - Select this to manually enter the DNS server used by the MAX208M2W Series.</li> </ul>
Static DHCP	
MAC Address	This field displays the MAC address of the static DHCP client connected to the MAX208M2W Series.
IP Address	This field displays the IP address of the static DHCP client connected to the MAX208M2W Series.
Add	Click this to add a new static DHCP entry.
OK	Click this to save any changes made to this list.
DHCP Leased Hosts	
MAC Address	This displays the MAC address of the DHCP leased host.
IP Address	This displays the IP address of the DHCP leased host.
Remaining Time	This displays the how much time is left on the host's lease.
Refresh	Click this to refresh the list.

## 7.8 WLAN

Use this screen to configure the connections between the MAX208M2W Series and the wireless clients that want to access the Internet.

Click **Network Setting > WLAN** to open this screen as shown next.

**Figure 40** WLAN Screen

The screenshot shows the WLAN configuration interface with the following fields:

- WiFi Settings**
  - Enable WLAN:
  - WLAN Mode: 802.11 B/G/N mixed
  - WLAN Channel: channel 11
  - WLAN Maximum STA number: 16 (1 ~ 16)
  - WLAN TxPower: default
- SSID Settings**
  - WLAN SSID: 319M2W\_PC7
  - Hide SSID:
  - Encryption Type: WPA Personal
- SSID WPA Settings**
  - WPA Mode: WPA
  - Cipher Type: TKIP
  - Pre-shared Key: [Redacted]

This screen contains the following fields:

**Table 28** Network Setting > WLAN

LABEL	DESCRIPTION
WiFi Settings	
Enable WLAN	Select this to activate the wireless LAN.
WLAN Mode	Select <b>802.11B/G mixed</b> to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the HES-219M2W. Select <b>802.11B only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HES-219M2W. Select <b>802.11A only</b> to allow only IEEE 802.11a compliant WLAN devices to associate with the HES-219M2W. Select <b>802.11G only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HES-219M2W.
WLAN Channel	Select this option and set the operating fequency/channel depending on your particular region. Select <b>Auto</b> to have the MAX208M2W Series scan and find an available channel.

**Table 28** Network Setting > WLAN

LABEL	DESCRIPTION
WLAN Maximum STA number	Enter the maximum number of wireless stations that is allowed to associate with the MAX208M2W Series.
WLAN TxPower	Select a number between 1 and 24 dB in the drop down box to control the strength of the connection signal, or leave it as <b>default</b> to let the MAX208M2W Series control this feature.
SSID Settings	
WLAN SSID	This field displays the name of the wireless network and it will appear to other computers that wish to connect wirelessly to the Internet.
Hide SSID	Select this to make the name of the network invisible to others.
Encryption Type	Select the type of encryption that the network will use: <b>None</b> , <b>WEP</b> or <b>WPA Personal</b> .
SSID WEP Settings	
Note: You will only see these options if you selected <b>WEP</b> as the Encryption Type	
Authentication Method	Select the type of authentication used to join the network: <b>OPEN SYSTEM</b> or <b>SHARED KEY</b> .
WEP Encryption Length	Select the length of the encryption key: 64-bit or 128-bit.
Key 1 - 4	Pick one of four available keys. The key can be in either HexaDecimal ( <b>HEX</b> ) or <b>ASCII</b> format.  Type the key using any letters and numbers. The field is case sensitive and the length must match the length picked in the step above (64-bit or 128-bit). A warning message will appear if you fail to do this.
SSID WPA Settings	
Note: You will only see these options if you selected <b>WPA Personal</b> as the Encryption Type.	
WPA Mode	Select either <b>WPA</b> , <b>WPA2</b> or <b>Auto (WPA or WPA2)</b> .
Cipher Type	Select the type of authentication that you wish to use for your network: <b>TKIP</b> , <b>AES</b> or <b>TKIP and AES</b> . AES is more secure.
Pre-shared Key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

## 7.9 WPS

Use this screen to configure WiFi Protected Setup (WPS) on your MAX208M2W Series.

WPS allows you to quickly set up a wireless network with strong security without having to configure security settings manually. Set up each WPS connection between two devices. Both devices have to support WPS.

Click **Network Setting > WLAN > WPS** to open this screen as shown next.

**Figure 41** WPS Screen



This screen contains the following fields:

**Table 29** WPS

LABEL	DESCRIPTION
Enable WPS	Select <b>Enable</b> and click <b>Apply</b> to activate WPS on the MAX208M2W Series. Select <b>Disable</b> and click <b>Apply</b> to deactivate WPS.
Start WPS PBC	This field is available after you select <b>Enable</b> in the <b>Enable WPS</b> field and click <b>Apply</b> .  Click this to activate the Push Button Configuration. After clicking this you will be able to use the WPS button at the back of the device to add new wireless clients.  Note: You must press the WPS buttons within two minutes of each other.

## 7.10 MAC Address Filter

Use these screens to configure a MAC (Media Access Control) address filter to restrict access to the network.



Click on **Network Setting > WLAN > MAC Address Filter**. The screen appears as shown.

**Figure 42** MAC Address Filter Screen

This screen contains the following fields:

**Table 30** MAC Address Filter

LABEL	DESCRIPTION
Enable MAC Address Filter	Select the check box to enable MAC address filtering. Then, the following fields display.
Mode	Define the filter action for the list of MAC addresses in the MAC address table.  Select <b>Allow listed stations</b> to permit access to the MAX208M2W Series only to addresses listed. MAC addresses not listed will be denied access to the MAX208M2W Series.  Select <b>Deny listed stations</b> to block access to the MAX208M2W Series to the computers or devices listed in this list.
#	This is the index number of the MAC address.
Active	Select this box to make the policy effective or ineffective for a particular device.
Name	Type the name of the device. The name can be up to 20 characters long, and any combination of letters, numbers or symbols.
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the MAX208M2W Series 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.
Delete	Click to delete a specific MAC address from the list.
Add	Click to add a MAC address to the list.
OK	Click this button when you are done adding a MAC Address.

## 7.11 Static Route

Use these settings to create fixed paths through the network.

Click **Network Setting > Route > Static Route** to open this screen as shown next.

**Figure 43** Static Route Screen

#	Destination	Subnet Mask	Next Hop	Metric
Total Num: 0				

This screen contains the following fields:

**Table 31** Static Route

LABEL	DESCRIPTION
Destination	This field displays the destination IP address of the static route.
Subnet Mask	This field displays the subnet mask of the static route.
Next Hop	This field displays next hop information of the static route.
Metric	This field displays the static route metric.
Add	Click this to add a new static route to the list.

## 7.12 Static Route Add

Use these settings to configure a static route.

Click **Add** in the **Network Setting > Route > Static Route** screen to open this screen as shown next.

**Figure 44** Static Route Screen

**Edit Static Route**

Destination IP: 0.0.0.0

Subnet Mask: 0.0.0.0

Next Hop:  Interface (WAN)  IP Address

Metric (1-255): 1

This screen contains the following fields:

**Table 32** Static Route

LABEL	DESCRIPTION
Destination IP	Enter the destination IP address of the static route.
Subnet Mask	Enter the subnet mask of the static route.
Next Hop	Select <b>Interface</b> and then select <b>WAN</b> or <b>LAN</b> for the next hop of the static route.  If the next hop is an IP address rather than an interface on the MAX208M2W Series, select <b>IP Address</b> and enter the IP address.
Metric	Enter the static route metric.

## 7.13 RIP

Use these settings to configure how the WiMAX Device exchanges information with other routers.

Click **Network Setting > Route > RIP** to open this screen as shown next.

**Figure 45** RIP Screen

**General Setup**

Enable

**Redistribute**

Active	Type	Metric(0~16)
Y	static route	7

Total Num: 1 [Edit] [OK]

**LAN**

Direction:

Version:

Authentication:

Authentication ID:

Authentication Key:

**WAN**

Direction:

Version:

Authentication:

Authentication ID:

Authentication Key:

This screen contains the following fields:

**Table 33** RIP

LABEL	DESCRIPTION
General Setup	
Enable	Select this to enable RIP on the MAX208M2W Series.
Redistribute	
Active	This indicates whether a route is being redistributed.
Type	This indicates what type of route is being redistributed.
Metric	This indicates the metric that is being used for redistribution.
Edit	Click this to edit a selected route.
OK	Click this to save any changes to the redistribution table.
LAN	
Direction	Set the LAN network direction to use with RIP.
Version	Set the RIP version to use.
Authentication	Use this option to enable or disable RIP authentication.
Authentication ID	Enter the authentication ID to use for RIP authentication.
Authentication Key	Enter the authentication key to use for RIP authentication.
WAN	
Direction	Set the WAN network direction to use with RIP.
Version	Set the RIP version to use.
Authentication	Use this option to enable or disable RIP authentication.
Authentication ID	Enter the authentication ID to use for RIP authentication.
Authentication Key	Enter the authentication key to use for RIP authentication.

## 7.14 Port Forwarding

Use these settings to forward incoming service requests to the ports on your local network.

Note: Make sure you did not configure a DMZ host in the **Network Setting > NAT > DMZ** screen if you want to make the settings of this screen work.

Click **Network Setting > NAT > Port Forwarding** to open this screen as shown next.

**Figure 46** Port Forwarding Screen

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP	
				Start Port	End Port	Start Port	End Port		
1	N	Name1	TCP	0	0	0	0	1.1.1.1	🗑️
2	N	Name2	TCP	0	0	0	0	1.1.1.1	🗑️
3	N	Name3	TCP	0	0	0	0	1.1.1.1	🗑️
4	N	Name4	TCP	0	0	0	0	1.1.1.1	🗑️
5	N	Name5	TCP	0	0	0	0	1.1.1.1	🗑️

Total Num: 5

Wizard Add OK

This screen contains the following fields:

**Table 34** Port Forwarding

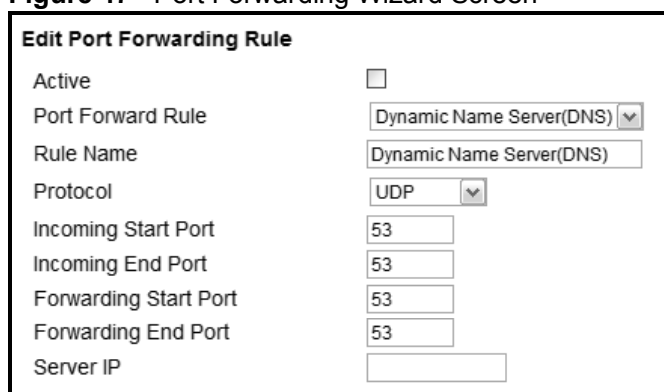
LABEL	DESCRIPTION
Active	This indicates whether the port forwarding rule is active or not.
Name	The displays the name of the port forwarding rule.
Protocol	This displays the protocol to which the port forwarding rule applies.
Incoming Port(s)	
Start Port	This displays the starting port number for incoming traffic for the port forwarding rule.
End Port	This displays the ending port number for incoming traffic for the port forwarding rule.
Forward Port(s)	
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 <b>Start Port</b> , only one port number is forwarded.
Server IP	This displays the IP address of the server to which packet for the selected port(s) are forwarded.
Delete	Click this to delete a specified rule.
Wizard	Click this to open the port forwarding "wizard".
Add	Click this to add a new port forwarding rule.
OK	Click this to save any changes made to the port forwarding list.

## 7.14.1 Port Forwarding Wizard

Use this wizard to set up a port forwarding rule for incoming service requests to the ports on your local network.

Click **Network Setting > NAT > Port Forwarding > Wizard** to open this screen as shown next.

**Figure 47** Port Forwarding Wizard Screen



This screen contains the following fields:

**Table 35** Port Forwarding Wizard

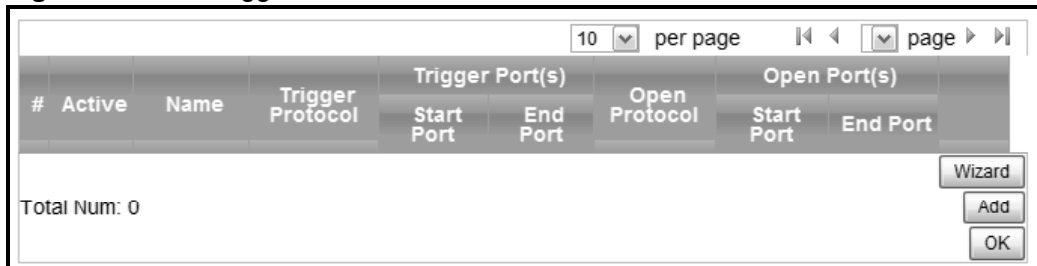
LABEL	DESCRIPTION
Active	Select this to make this port forwarding rule active.
Port Forward Rule	Select the type of port forwarding rule.
Rule Name	Enter a name for the port forwarding rule.
Protocol	Select the port forwarding protocol.
Incoming Start Port	Enter the starting port number for incoming traffic for the port forwarding rule.
Incoming End Port	Enter the ending port number for incoming traffic for the port forwarding rule.
Forwarding Start Port	Enter the starting port number for forwarded traffic for the port forwarding rule.
Forwarding End Port	Enter the ending port number for forwarded traffic for the port forwarding rule.
Server IP	Enter the port forwarding server IP address.

## 7.15 Port Trigger

Use these settings to automate port forwarding and allow computers on local network to provide services that would normally require a fixed address on the local network.

Click **Network Setting > NAT > Port Trigger** to open this screen as shown next.

**Figure 48** Port Trigger Screen



This screen contains the following fields:

**Table 36** Port Trigger

LABEL	DESCRIPTION
Active	This indicates whether the port trigger rule is active or not.
Name	The displays the name of the port trigger rule.
Trigger Protocol	This displays the protocol to which the port trigger rule applies.
Trigger Port(s)	
Start / End Port	<p>This displays the start / end trigger port for the port trigger rule.</p> <p>Click <b>Add</b> to create a new, empty rule, then enter the incoming port number or range of port numbers you want to forward to the IP address the MAX208M2W Series records.</p> <p>To forward one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields.</p> <p>To forward a range of ports,</p> <ul style="list-style-type: none"> <li>enter the port number at the beginning of the range in the <b>Start Port</b> field</li> <li>enter the port number at the end of the range in the <b>End Port</b> field.</li> </ul> <p>If you want to delete this rule, click the <b>Delete</b> icon.</p>
Open Protocol	This indicates which protocol is used to open the port trigger ports.
Open Port(s)	

**Table 36** Port Trigger (continued)

LABEL	DESCRIPTION
Start / End Port	<p>This displays the start / end open port for the port trigger rule.</p> <p>Click <b>Add</b> to create a new, empty rule, then enter the outgoing port number or range of port numbers that makes the MAX208M2W Series record the source IP address and assign it to the selected incoming port number(s).</p> <p>To select one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields.</p> <p>To select a range of ports,</p> <ul style="list-style-type: none"> <li>enter the port number at the beginning of the range in the <b>Start Port</b> field</li> <li>enter the port number at the end of the range in the <b>End Port</b> field.</li> </ul> <p>If you want to delete this rule, click the <b>Delete</b> icon.</p>
Delete	Click this to delete a specified rule.
Wizard	Click this to open the port trigger "wizard".
Add	Click this to add a new port trigger rule.
OK	Click this to save any changes made to the port trigger list.

### 7.15.1 Port Trigger Wizard

Use the wizard to create a port trigger rules that will allow the MAX208M2W Series to to automate port forwarding and allow computers on local network to provide services that would normally require a fixed address on the local network.

Click Network Setting > NAT > Port Trigger > Wizard

**Figure 49** Port Trigger Wizard Screen

**Edit Port Trigger Rule**

Active

Port Trigger Rule

Rule Name

Trigger Protocol

Trigger Start Port

Trigger End Port

Open Protocol

Open Start Port

Open End Port



This screen contains the following fields:

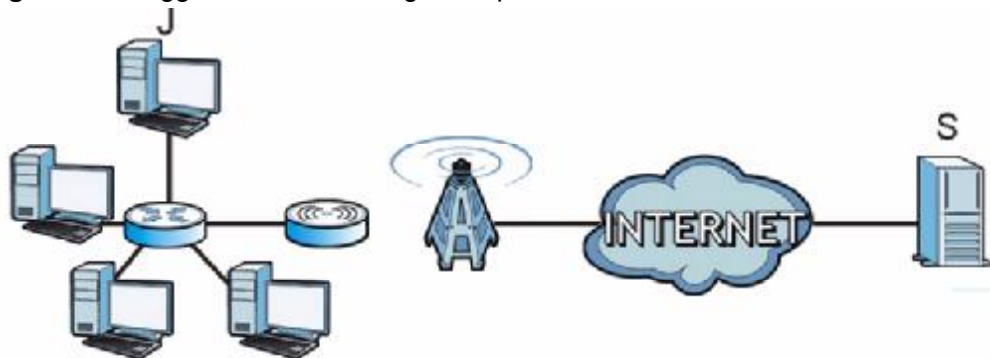
**Table 37** Port Trigger Wizard

LABEL	DESCRIPTION
Active	Select this to make this port trigger rule active.
Port Trigger Rule	Select the type of port trigger rule.
Rule Name	Enter a name for the port trigger rule.
Trigger Protocol	Select the type of port trigger protocol.
Trigger Start Port	Enter the port trigger start port.
Trigger End Port	Enter the port trigger end port.
Open Protocol	Select the type of open protocol for the port trigger rule.
Open Start Port	Select the starting open port for the port trigger rule.
Open End Port	Select the ending open port number for the port trigger rule.

## 7.15.2 Trigger Port Forwarding Example

The following is an example of trigger port forwarding. In this example, **J** is Jane's computer and **S** is the Real Audio server.

**Figure 50** Trigger Port Forwarding Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the MAX208M2W Series to record Jane's computer IP address. The MAX208M2W Series associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The MAX208M2W Series forwards the traffic to Jane's computer IP address.

- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The MAX208M2W Series times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Two points to remember about trigger ports:

- 1 Trigger events only happen on data that is coming from inside the MAX208M2W Series and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

## 7.16 DMZ

Use this page to set the IP address of your network DMZ (if you have one) for the WiMAX Device. All incoming packets received by this MAX208M2W Series's WAN interface will be forwarded to the DMZ host you set.

Click **Network Setting > NAT > DMZ** to open this screen as shown next.

Note: The configuration you set in this screen takes priority than the **Network Setting > NAT > Port Forwarding** screen.

**Figure 51** DMZ Screen

The screenshot shows a configuration screen for DMZ. It features a single text input field with the label "DMZ Host" on the left and the value "0.0.0.0" entered in the field on the right.

This screen contains the following fields:

**Table 38** DMZ

LABEL	DESCRIPTION
DMZ Host	Enter the IP address of your network DMZ host, if you have one. <b>0.0.0.0</b> means this feature is disabled.

## 7.17 ALG

Use these settings to bypass NAT on your WiMAX Device for those applications that are "NAT un-friendly".

Click **Network Setting > NAT > ALG** to open this screen as shown next.

**Figure 52** ALG Screen

Enable FTP ALG	<input checked="" type="checkbox"/>
Enable H.323 ALG	<input checked="" type="checkbox"/>
Enable IPsec ALG	<input checked="" type="checkbox"/> <i>(Allow IPsec pass through)</i>
Enable L2TP ALG	<input checked="" type="checkbox"/> <i>(Allow L2TP pass through)</i>
Enable PPTP ALG	<input checked="" type="checkbox"/> <i>(Allow PPTP pass through)</i>
Enable RTSP ALG	<input checked="" type="checkbox"/> <i>(Allow RTSP pass through)</i>
Enable SIP ALG	<input checked="" type="checkbox"/>
SIP Port	<input type="text" value="5060"/>
Enable SIP ALG Set BSID	<input type="checkbox"/>

This screen contains the following fields:

**Table 39** Network Setting > NAT > ALG

LABEL	DESCRIPTION
Enable FTP ALG	Turns on the FTP ALG to detect FTP (File Transfer Program) traffic and helps build FTP sessions through the MAX208M2W Series's NAT.
Enable H.323 ALG	Turns on the H.323 ALG to detect H.323 traffic (used for audio communications) and helps build H.323 sessions through the MAX208M2W Series's NAT.
Enable IPsec ALG	Turns on the IPsec ALG to detect IPsec traffic and helps build IPsec sessions through the MAX208M2W Series's NAT.
Enable L2TP ALG	Turns on the L2TP ALG to detect L2TP traffic and helps build L2TP sessions through the MAX208M2W Series's NAT.
Enable PPTP ALG	Turns on the PPTP ALG to detect PPTP traffic and helps build PPTP sessions through the MAX208M2W Series's NAT.
Enable RTSP ALG	Turns on the RTSP ALG to detect RTSP traffic and helps build RTSP sessions through the MAX208M2W Series's NAT.
Enable SIP ALG	Turns on the SIP ALG to detect SIP traffic and helps build SIP sessions through the MAX208M2W Series's NAT.
SIP Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.
Enable SIP ALG Set BSID	Check this box to add the base station ID to the outgoing SIP messages. Select this option only if the media server forwarding calls requires this information.

## 7.18 UPnP

Use this page to enable the UPnP networking protocol on your WiMAX Device and allow easy network connectivity with other UPnP-compatible devices.

Click **Network Setting > UPnP** to open this screen as shown next.

**Figure 53** UPnP Screen

Enable UPnP	<input type="checkbox"/>
Enable NAT-PMP	<input type="checkbox"/>

This screen contains the following fields:

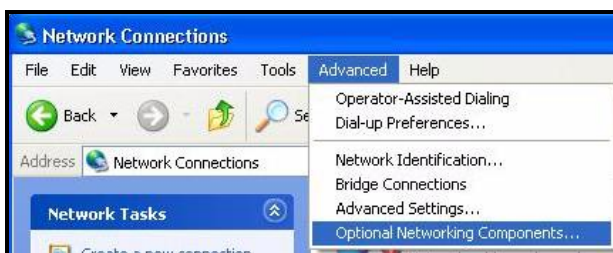
**Table 40** UPnP

LABEL	DESCRIPTION
Enable UPnP	Select this to enable UPnP on the MAX208M2W Series.
Enable NAT-PMP	Select this to enable NAT Port Mapping Protocol on the MAX208M2W Series.

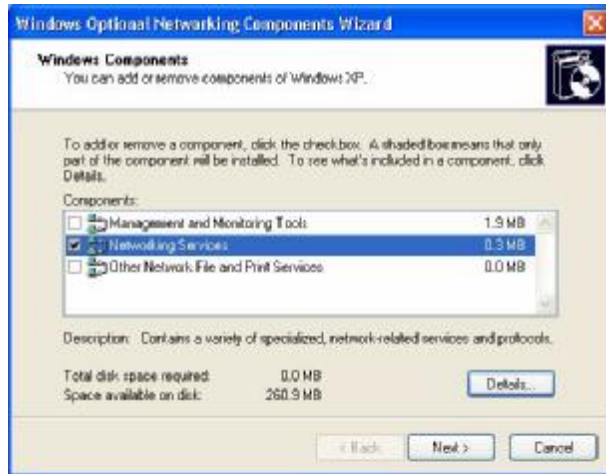
### 7.18.1 Installing UPnP in Windows XP

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

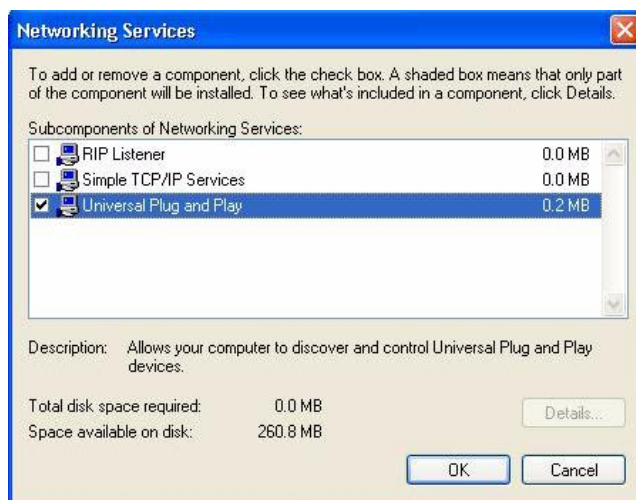
- 1 Click **Start > Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**



- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.



- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

### 7.18.1.1 Auto-discover Your UPnP-enabled Network Device in Windows XP

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the MAX208M2W Series.

Make sure the computer is connected to a LAN port of the MAX208M2W Series. Turn on your computer and the MAX208M2W Series.

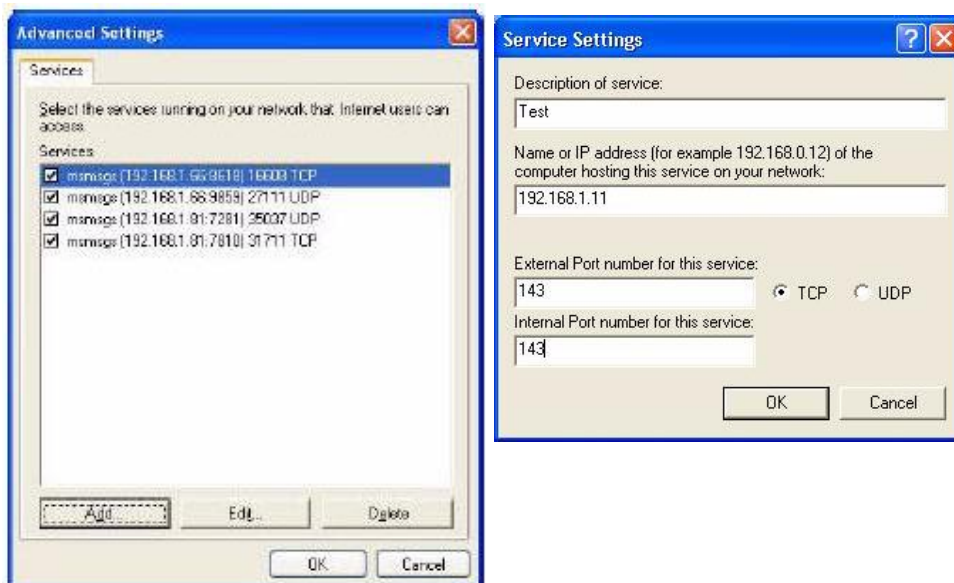
- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.



- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.



- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.



- 7 Double-click on the icon to display your current Internet connection status.



## 7.18.2 Web Configurator Easy Access

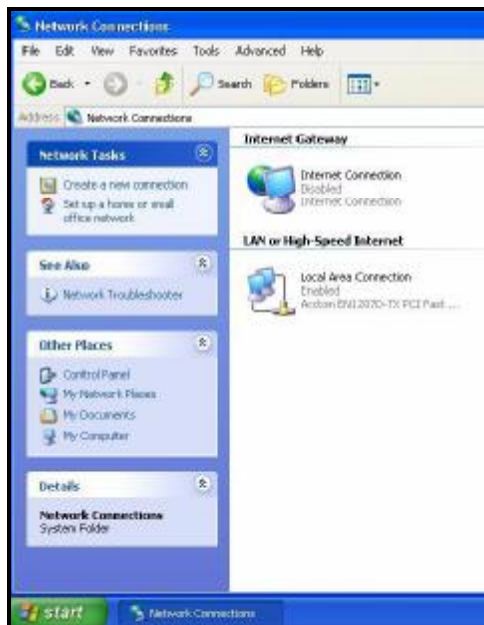
With UPnP, you can access the web-based configurator on the MAX208M2W Series without finding out the IP address of the MAX208M2W Series first. This becomes helpful if you do not know the IP address of the MAX208M2W Series.

Follow the steps below to access the web configurator:

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.



3 Select **My Network Places** under **Other Places**.



4 An icon with the description for each UPNP-enabled device displays under **Local Network**.

5 Right-click on the icon for your MAX208M2W Series and select **Invoke**. The web configurator login screen displays.



- 6 Right-click on the icon for your MAX208M2W Series and select **Properties**. A properties window displays with basic information about the MAX208M2W Series.



## 7.19 VLAN

Use this screen to configure port-based VLAN settings on the MAX208M2W Series. This screen allows you to assign port(s) to specific virtual LAN(s) in order to isolate traffic from different VLAN groups.

Click **Network Setting > VLAN** to open the screen as shown next.

**Figure 54** VLAN Screen

**Management VLAN**

VLAN ID

Priority

Port Egress Tagging

#	Tag
1	untagged
2	untagged

Total Num: 2 OK

**Port Settings**

10 per page    1 page

#	PVID Group	Priority
1	1	0
2	1	0

Total Num: 2 OK

**VLAN Rules**

10 per page    1 page

#	VID	Port 1		Port 2	
		Join	Tag	Join	Tag
1	1	Y	untagged	Y	untagged
2	2	Y	untagged	Y	untagged
3	3	Y	untagged	Y	untagged
4	4	Y	untagged	Y	untagged
5	5	Y	untagged	Y	untagged
6	6	Y	untagged	Y	untagged
7	7	Y	untagged	Y	untagged

Total Num: 7 OK

This screen contains the following fields:

**Table 41** VLAN

LABEL	DESCRIPTION
Management VLAN	
VLAN ID	Enter an ID number (1~4094) to create a new VLAN. Enter 0 to disable VLAN on the MAX208M2W Series.  Note: To use VLAN on the MAX208M2W Series, you must switch the operation mode to “bridge” on the <b>Network Setting &gt; WAN</b> screen. It will then require system restart to take effect.
Priority	Enter a priority level (1~7) that the MAX208M2W Series assigns to frames belonging to this VLAN. Enter “0” for no priority assigned.
Port Egress Tagging	
#	This is the index number of a port (1 or 2).

**Table 41** VLAN

LABEL	DESCRIPTION
Tag	This field displays whether to prioritize traffic transmitted by the port, <b>tagged</b> or <b>untagged</b> . Click this field to change the setting. Set this to untagged if you do not want to prioritize outgoing traffic through the port.
OK	Click this to save the changes in the <b>Port Egress Tagging</b> section.
Port Settings	
#	This is the index number of a port (1 or 2).
PVID Group	This field displays the index number of a VLAN rule with which the port is associated. Click this field to change the setting. Select <b>MGMT</b> to allow the computer(s) connected to the port to access the MAX208M2W Series using the LAN IP address (see the <b>Network Setting &gt; LAN &gt; IP</b> screen).  Note: Set one port to <b>MGMT</b> so that you can still manage the MAX208M2W Series through the port. Set both ports to <b>tagged</b> if you do not need to manage the MAX208M2W Series any more.
Priority	Enter a priority level (1~7) that the MAX208M2W Series assigns to frames belonging to this VLAN. Enter "0" for no priority assigned.
OK	Click this to save the changes in the <b>Port Settings</b> section.
VLAN Rules - You can configure up to 7 VLANs on the MAX208M2W Series. By default, VLANs 1 to 7 are configured.	
#	This is the index number of a VLAN rule.
VID	This field displays the VLAN ID of the VLAN rule. Click this field to change the VLAN ID. When you make the change, make sure you configure the same VLAN ID in the <b>Management VLAN</b> section..
Port1 / Port 2	This is an indicator of which port is being configured.
Join	Select <b>Y</b> to add the port into the VLAN group. Otherwise, select <b>N</b> .
Tag	This field displays the allowed traffic for the port, VLAN- <b>tagged</b> or VLAN- <b>untagged</b> . Click this field to change the setting.
OK	Click this to save the changes in the <b>VLAN Rules</b> section.

## 7.20 DDNS

Use this page to configure the WIMAX Device as a dynamic DNS client.

Click Network Setting > DDNS

**Figure 55** DDNS Screen

Enable Dynamic DNS	<input type="checkbox"/>
Service Provider	dyndns.org(www.dyndns.org) ▼
Service Type	Dynamic ▼
Domain Name	<input type="text"/> . <input type="text"/>
Login Name	<input type="text"/>
Password	<input type="text"/>
IP Update Policy	Auto Detect ▼
User Defined IP	<input type="text"/>
Wildcards	<input type="checkbox"/>
MX	<input type="checkbox"/>
Backup MX	<input type="checkbox"/>
MX Host	<input type="text"/>

This screen contains the following fields:

**Table 42** DDNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this to enable dynamic DNS on the MAX208M2W Series.
Service Provider	Select the dynamic DNS service provider for the MAX208M2W Series.
Service Type	Select the dynamic DNS service type.
Domain Name	Enter the domain name.
Login Name	Enter the user name.
Password	Enter the password.
IP Update Policy	Select the policy used by the MAX208M2W Series. Options are: <ul style="list-style-type: none"> <li>• Auto Detect</li> <li>• WAN</li> <li>• User Defined</li> </ul>
User Defined IP	If chose "User Defined" for the <b>IP Update Policy</b> , enter the user defined IP address.
Wildcards	Select this to allow a hostname to use wildcards such as "*".
MX	Select this to enable mail routing, if supported by the specified DYNDNS service provider.

**Table 42** DDNS (continued)

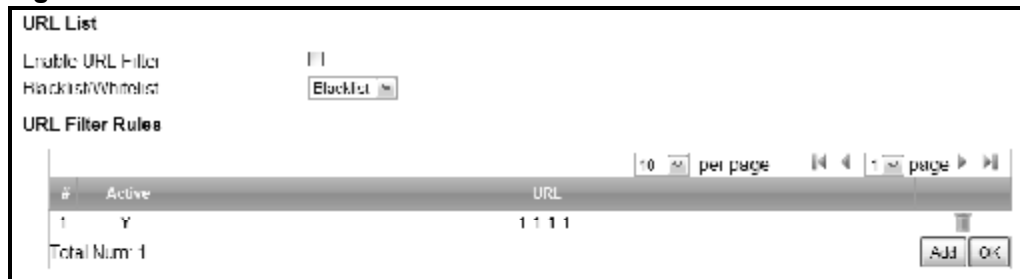
LABEL	DESCRIPTION
Backup MX	Select this to enable a secondary mail routing, if supported by the specified DYNDNS service provider.
MX Host	Enter the host to which mail is routed when the MX option is selected.

## 7.21 Content Filter

Use these settings to allow ("whitelist") or block ("blacklist") connections to and from specific web sites through the WiMAX Device.

Click **Network Setting > Content Filter** to open this screen as shown next.

**Figure 56** Content Filter Screen



This screen contains the following fields:

**Table 43** Content Filter

LABEL	DESCRIPTION
URL List	
Enable URL Filter	Select this employ the content filter to allow ("whitelist") or block ("blacklist") specific URL connections made through the MAX208M2W Series.
Blacklist/Whitelist	Select whether the current filtering applies to the blacklist (sites that are blocked) or the whitelist (sites that are allowed).
URL Filter Rule	
Active	Indicates whether the current URL filter is active or not.
URL	Indicates the URL to be filtered according to blacklist or whitelist rules.
Delete	Click this to delete a specified rule.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

# 8

## Security

### 8.1 Overview

This chapter shows you how to configure the MAX208M2W Series's network settings.

#### 8.1.1 What You Need to Know

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

##### **About the MAX208M2W Series's Security Features**

The MAX208M2W Series security features are designed to protect against Denial of Service attacks when activated as well as block access to and from specific URLs and MAC addresses. Its purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The MAX208M2W Series can be used to prevent theft, destruction and modification of data.

The MAX208M2W Series 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 MAX208M2W Series 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.

## 8.2 IP Filter

Use this screen to block incoming connections from specific IP addresses.

Click **Security > Firewall > IP Filter** to open this screen as shown next.

**Figure 57** IP Filter Screen



This screen contains the following fields:

**Table 44** IP Filter

LABEL	DESCRIPTION
Active	Indicates whether the current IP filter is active or not.
Source IP	This displays the source IP address for the IP filter rule. Click <b>Add</b> to create a new, empty rule, then enter the incoming IP address for the MAX208M2W Series to block. If you want to delete this rule, click the <b>Delete</b> icon.
Source Port	This displays the source port number for the IP filter rule. Click <b>Add</b> to create a new, empty rule, then enter the incoming port number for the MAX208M2W Series to block. If you want to delete this rule, click the <b>Delete</b> icon.
Destination IP	This displays the destination IP address for the IP filter rule. Click <b>Add</b> to create a new, empty rule, then enter the outgoing IP address for the MAX208M2W Series to block. If you want to delete this rule, click the <b>Delete</b> icon.
Destination Port	This displays the destination port number for the IP filter rule. Click <b>Add</b> to create a new, empty rule, then enter the outgoing port number for the MAX208M2W Series to block. If you want to delete this rule, click the <b>Delete</b> icon.
Protocol	This displays the protocol blocked by the IP filter rule. Click <b>Add</b> to create a new, empty rule, then select the protocol type for the MAX208M2W Series to block. If you want to delete this rule, click the <b>Delete</b> icon.
Delete	Click this to delete a specified rule.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.



## 8.3 MAC Filter

Use this screen to allow ("whitelist") or block ("blacklist") connections to and from specific devices on the network based on their unique MAC addresses.

Note: This feature only works when the MAX208M2W Series is in bridge mode.

Click **Security > Firewall > MAC Filter** to open this screen as shown next.

**Figure 58** MAC Filter Screen

This screen contains the following fields:

**Table 45** MAC Filter

LABEL	DESCRIPTION
Blacklist/ Whitelist	Select either whitelist or blacklist for viewing and editing.
Source MAC	This displays the source MAC for the MAC filter rule.  Click <b>Add</b> to create a new, empty rule, then enter the incoming MAC address for the MAX208M2W Series to block.  If you want to delete this rule, click the <b>Delete</b> icon.
Destination MAC	This displays the destination MAC for the MAC filter rule.  Click <b>Add</b> to create a new, empty rule, then enter the outgoing MAC address for the MAX208M2W Series to block.  If you want to delete this rule, click the <b>Delete</b> icon.
Mon ~ Sun	Select which days of the week you want the filter rule to be effective.
Start / End Time	Select what time each day you want the filter rule to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

## 8.4 DDOS

Use these settings to potentially block specific types of Denial of Service attacks directed at your WiMAX Device.

Click **Security > Firewall > DDOS** to open this screen as shown next.

**Figure 59** DDOS Screen

Prevent from TCP SYN Flood	<input type="checkbox"/>
Prevent from UDP Flood	<input type="checkbox"/>
Prevent from ICMP Flood	<input type="checkbox"/>
Prevent from Port Scan	<input type="checkbox"/>
Prevent from LAND Attack	<input type="checkbox"/>
Prevent from IP Spoof	<input type="checkbox"/>
Prevent from ICMP redirect	<input type="checkbox"/>
Prevent from PING of Death	<input type="checkbox"/>
Prevent from PING from WAN	<input type="checkbox"/>

This screen contains the following fields:

**Table 46** DDOS

LABEL	DESCRIPTION
Prevent from TCP SYN Flood	Select this to monitor for and block TCP SYN flood attacks. A SYN flood is one type of denial of service attack where an overwhelming number of SYN requests assault a client device.
Prevent from UDP Flood	Select this to monitor for and block UDP flood attacks. An UDP flood is a type of denial of service attack where an overwhelming number of UDP packets assault random ports on a client device. Because the device is forced to analyze and respond to each packet, it quickly becomes unreachable to other devices.
Prevent from ICMP Flood	Select this to monitor for and block ICMP flood attacks. An ICMP flood is a type of denial of service attack where an overwhelming number of ICMP ping assault a client device, locking it down and preventing it from responding to requests from other servers.
Prevent from Port Scan	Select this to monitor for and block port scan attacks. A port scan attack is typically the precursor to a full-blown denial of service attack wherein each port on a device is probed for security holes that can be exploited. Once a security flaw is discovered, an attacker can initiate the appropriate denial of service attack or intrusion attack against the client device.
Prevent from LAND Attack	Select this to monitor for and block LAND attacks. A Local Area Network Denial (LAND) attack is a type of denial of service attack where a spoofed TCP SYN packet targets a client device's IP address and forces it into an infinite recursive loop of querying itself and then replying, effectively locking it down.

**Table 46** DDOS (continued)

LABEL	DESCRIPTION
Prevent from IP Spoof	Select this to monitor for and block IP address spoof attacks.  An IP address spoof is an attack whereby the source IP address in the incoming IP packets allows a malicious party to masquerade as a legitimate user and gain access to the client device.
Prevent from ICMP redirect	Select this to monitor for and block ICMP redirect attacks.  An ICMP redirect attack is one where forged ICMP redirect messages can force the client device to route packets for certain connections through an attacker's host.
Prevent from PING of Death	Select this to monitor for and block ping of death attacks.  A Ping of Death (POD) attack is one where larger-than-allowed ping packets are fragmented then sent against a client device. This results in the client device suffering from a buffer overflow and subsequent system crash.
Prevent from PING from WAN	Select this to ignore ping requests from the WAN.



# The VoIP General Screens

## 9.1 VoIP Overview

The **VOICE > General** screens allow you to set up global SIP and Quality of Service (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.

### 9.1.1 What You Can Do in This Chapter

- The **Media** screen ([Section 9.2 on page 135](#)) lets you set up and maintain global VoIP settings on the MAX208M2W Series.
- The **QoS** screen ([Section 9.2 on page 135](#)) lets you set up and maintain QoS settings for voice traffic flowing through the MAX208M2W Series.

### 9.1.2 What You Need to Know

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

#### Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The MAX208M2W Series 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.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.

### Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay and the networking methods used to provide bandwidth for real-time multimedia applications.

### Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the MAX208M2W Series) so a server can decide the best method of delivery, that is the least cost, fastest route and so on. The ToS field is consist of 8 bits. The first 3 bits indicate the priority of the packet.

### 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.

DiffServ uses the first 6 bits of the 8-bit ToS value so that it can backward compatible with non-DiffServ compliant but ToS-enabled network device. See [Section 9.3.1 on page 137](#) for more information.

### 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.

## 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.

### 9.1.3 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 MAX208M2W Series.
- Connect your MAX208M2W Series 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.

## 9.2 Media

Click **VoIP > General > Media** to set up and maintain global VoIP settings.

**Figure 60** VoIP > General > Media

<b>Port Range</b>	
Media Port Start	<input type="text" value="40000"/> (40000~50000, default:40000)
Media Port End	<input type="text" value="50000"/> (40000~50000, default:50000)
<b>Codec Packetization Time Settings</b>	
G.711	<input type="text" value="20"/> <input type="button" value="v"/> msec
G.729	<input type="text" value="20"/> <input type="button" value="v"/> msec
<b>Advanced</b>	
Voice Jitter Buffer Type	<input type="text" value="Dynamic"/> <input type="button" value="v"/>
Voice Jitter Buffer Length	<input type="text" value="120"/> msec (120~500 ms, default:120)
Packet Loss Concealment	<input checked="" type="checkbox"/>
T.38 Static Jitter Length	<input type="text" value="210"/> msec (80~500 ms, default:210)

The following table describes the labels in this screen.

**Table 47** VoIP > General > Media

LABEL	DESCRIPTION
Port Range	
Media Port Start Media Port End	<p>Enter the listening port number(s) for RTP traffic on the MAX208M2W Series, 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 both <b>Media Port Start</b> and <b>Media Port End</b> fields.</p> <p>To enter a range of ports, enter the beginning port number of the range in the <b>Media Port Start</b> field and the ending port number in the <b>Media Port End</b> field.</p>
Codec Packetization Time Settings	
G.711, G.729	Select the type of voice coder/decoder (codec) that you want the MAX208M2W Series to use. <b>G.711</b> provides high voice quality but requires more bandwidth (64 kbps). <b>G.729</b> requires only 8 kbps.
Advanced	
Voice Jitter Buffer Type	<p>Voice jitter is a variation in delay of RTP packets delivery. This could cause strange sound effects. The MAX208M2W Series can utilize the following types of jitter buffer to minimize the effects of jitter.</p> <p><b>Dynamic</b> - Jitter buffer size is dynamically changed by RTP packets delivery status.</p> <p><b>Static</b> - Jitter buffer size is fixed.</p>
Voice Jitter Buffer Length	Select the maximum number of milliseconds of voice traffic the MAX208M2W Series can help to smooth out the jitter in order to ensure good voice quality for your conversations.
Packet Loss Concealment	Packets may be dropped due to an overwhelming amount of traffic on the network. Some degree of packet loss will not be noticeable to the end user, but as packet loss increases the quality of sound degrades. Select this to have the MAX208M2W Series to improve the voice quality when packet loss occurs.
T.38 Static Jitter Length	<p>T.38 is an ITU-T standard that VoIP devices use to send fax messages over the Internet.</p> <p>Select the number of milliseconds for the jitter buffer size used for transmitting T.38 fax messages.</p>

## 9.2.1 QoS

This section describes the features of the Quality of Service (QoS) screen.



## 9.2.2 QoS Settings

Click **VoIP > General > QoS** to set up Type of Service (ToS) and Differentiated Services (DiffServ) settings for voice traffic transmission through the MAX208M2W Series.

**Figure 61** VoIP > General > QoS

SIP ToS / DiffServ	<input type="text" value="0x2E"/>
RTP ToS / DiffServ	<input type="text" value="0x38"/>

The following table describes the labels in this screen.

**Table 48** VoIP > General > QoS

LABEL	DESCRIPTION
SIP ToS/ DiffServ	Enter the first 6 bits of the ToS field in hexadecimal (in a format of 0x00), which you want to mark on all outgoing SIP packets flowing through the MAX208M2W Series. The MAX208M2W Series automatically converts this number to another in order to compatible with DiffServ-enabled network. For example, if you enter 0x2E, it is 101110 in binary for ToS service. The MAX208M2W Series converts it to 101110 <u>00</u> in binary for DiffServ-enabled network.
RTP ToS/ DiffServ	Select the ToS value in hexadecimal (in a format of 0x00) to mark all outgoing RTP packets flowing through the MAX208M2W Series.

## 9.3 Technical Reference

The following section contains additional technical information about the MAX208M2W Series features described in this chapter.

### 9.3.1 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 62** 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 VoIP Account Screens

## 10.1 Overview

Use the **VoIP > Account 1** and **VoIP > Account 2** screens to configure SIP servers, authentication, additional VoIP features, dialing timeout values, speed-dial rules and how to handle fax messages for two accounts on the MAX208M2W Series. Account 1 maps to phone port 1 and account 2 maps to phone port 2. Since both the **Account 1** and **Account 2** screens are quite similar, this section uses the **VoIP > Account 1** screens to describe the fields.

### 10.1.1 What You Can Do in This Chapter

- The **Status** screen ([Section 10.2 on page 144](#)) lets you view the current status of the SIP server, STUN server, selected phone line and call history. You can also manually disconnect the VoIP connection or request the SIP server for a new connection.
- The **Server** screen ([Section 10.3 on page 146](#)) lets you configure the SIP server, proxy server, outbound server and STUN server settings for the phone line.
- The **Feature** screen ([Section 10.4 on page 147](#)) lets you configure the SIP additional functions such as DTMF, call forward, call waiting and hotline settings for the phone line.
- The **User** screen ([Section 10.5 on page 150](#)) lets you configure the SIP account, codec and SIP settings for the phone line.
- The **Dialing** screen ([Section 10.6 on page 152](#)) lets you configure some timeout setting for the phone line.
- The **Speed Dial** screen ([Section 10.7 on page 152](#)) lets you add, edit, or remove speed-dial entries for the phone line.
- The **FAX** screen ([Section 10.8 on page 153](#)) lets you configure which standard the phone line uses for sending FAXes.

### 10.1.2 What You Need to Know

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

## 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](mailto:johndoe@your-ITSP.com) for example) or numbers like a telephone number ([1122334455@VoIP-provider.com](tel: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](tel:1122334455@VoIP-provider.com), then "VoIP-provider.com" is the SIP service domain.

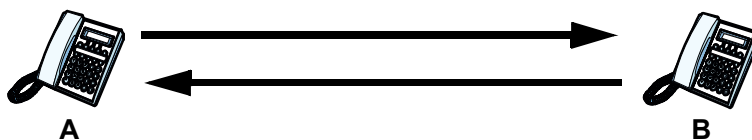
## SIP Register Server

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.

### 10.1.3 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 63** SIP User Agent



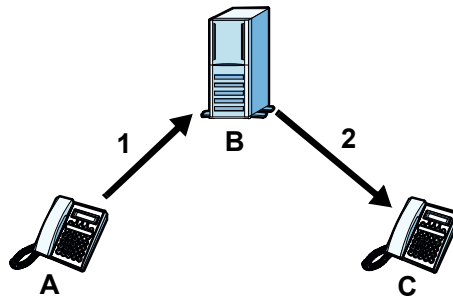
## SIP Proxy Server

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 64** SIP Proxy Server



## STUN

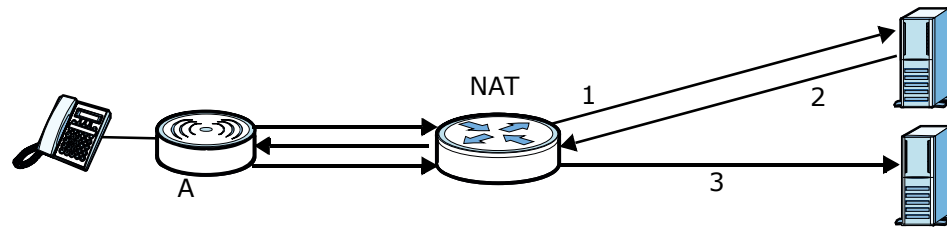
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the MAX208M2W Series to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the MAX208M2W Series to find the public IP address that NAT assigned, so the MAX208M2W Series can embed it in the SIP data stream. STUN does not work with symmetric NAT routers or firewalls. See RFC 3489 for details on STUN.

The following figure shows how STUN works.

- 1 The MAX208M2W Series (**A**) sends SIP packets to the STUN server (**B**).
- 2 The STUN server (**B**) finds the public IP address and port number that the NAT router used on the MAX208M2W Series's SIP packets and sends them to the MAX208M2W Series.

- 3 The MAX208M2W Series uses the public IP address and port number in the SIP packets that it sends to the SIP server (C).

**Figure 65** STUN



### Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the MAX208M2W Series's VoIP traffic. This allows the MAX208M2W Series to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the MAX208M2W Series to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).

### NAT and SIP

The MAX208M2W Series must register its public IP address with a SIP register server. If there is a NAT router between the MAX208M2W Series and the SIP register server, the MAX208M2W Series probably has a private IP address. The MAX208M2W Series 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 MAX208M2W Series's IP address from inside the SIP message and maps it to your SIP identity. If the MAX208M2W Series has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity.

Use a SIP ALG (Application Layer Gateway), STUN, or outbound proxy to allow the MAX208M2W Series to list its public IP address in the SIP messages.

### Speed Dial and Peer-to-Peer Calling

Speed dial provides shortcuts for dialing frequently used phone numbers. You can map a phone number to an alphanumeric keypad key (**1** to **9**) and then use that keypad key to call the phone number (press and hold the key for one second or longer). Use this screen to add, edit, or remove speed-dial numbers for outgoing calls.

You also have to create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that use letters.

In peer-to-peer calls, you call another VoIP device directly without going through a SIP server. Enter the callee's IP address or domain name. The MAX208M2W Series 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.

## **DTMF**

Dual-Tone Multi-Frequency (DTMF) telephone call signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

## **Supplementary Phone Services Overview**

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The MAX208M2W Series supports the following services:

- Call Waiting
- Call Forwarding
- Caller ID
- Hotline

**Note:** To take full advantage of the supplementary phone services available through the MAX208M2W Series's phone port, you may need to subscribe to the services from your VoIP service provider.

## 10.2 Status

Click **VoIP > Account 1 (or Account 2) > Status** to view VoIP settings and current status.

**Figure 66** VoIP > Account 1 (or Account 2) > Status

Server Status	
SIP Registrar	192.168.2.200:5060
SIP Service Domain	192.168.2.200:5060
Proxy Server	192.160.2.200:5060
Outbound Server	192.160.2.200:5060
Register Status	Unregistered
STUN Status	
STUN Server	192.160.2.200:3478
STUN Status	Enable
Line Status	
Subscriber Number	1000
Account Status	Enable
Phone Status	Idle
Call History	
Received call	0
Missing call	0
Outgoing call	0
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	

The following table describes the labels in this screen.

**Table 49** VoIP > Account 1 (or Account 2) > Status

LABEL	DESCRIPTION
Server Status	
SIP Register	This field displays the IP address and service port number of the SIP register server, if you have configured one.
SIP Service Domain	This field displays the IP address and service port number of the second SIP register server, if you have configured one.
Proxy Server	This field displays the IP address and service port number of the SIP proxy server, if you have configured one.
Outbound Server	This field displays the IP address and service port number of the outbound proxy server, if you have configured one.
Register Status	This field displays <b>Registered</b> , if the connected phone is registered with the register server. It displays <b>Unregistered</b> if the phone has not registered successfully to the register server yet.
STUN Status - see <a href="#">STUN on page 141</a>	



**Table 49** VoIP > Account 1 (or Account 2) > Status

LABEL	DESCRIPTION
STUN Server	This field displays the IP address and service port number of the STUN (Simple Traversal of UDP through NATs (Network Address Translation)) server, if you have configured one.
STUN Status	This field displays whether you have enabled STUN server support on the MAX208M2W Series.
Line Status	
Subscriber Number	This field displays the SIP phone number for the phone line.
Account Status	This indicates whether the SIP account is activated or not, or if it is unspecified for the phone line.
Phone Status	This field displays <b>busy</b> if the SIP phone number is currently engaged, otherwise it displays <b>idle</b> .
Call History	
Received call	This field displays the number of calls you have received through the connected phone since the MAX208M2W Series last restarted or was turned on.
Missing call	This field displays the number of calls you have missed since the MAX208M2W Series last restarted or was turned on.
Outgoing call	This field displays the number of calls you have made through the connected phone since the MAX208M2W Series last restarted or was turned on.
Connect	Click this to register the MAX208M2W Series to the specified register server.
Disconnect	Click this to disconnect the connected phone with the register server.

## 10.3 Server

Click **VoIP > Account 1 (or Account 2) > Server** to configure the register server, proxy server, outbound proxy server and NAT settings for this SIP account.

**Figure 67** VoIP > Account 1 (or Account 2) > Server

<b>Registrar Server</b>	
Registrar Server	192.168.2.200
Port Number	5060
SIP Service Domain	192.168.2.200
Registrar Period Time	300 seconds (60~65535, default 300)
<b>Proxy Server</b>	
Proxy Server	192.168.2.200
Port Number	5060
<b>Outbound Server</b>	
Outbound Server	192.168.2.200
Port Number	5060
<b>NAT Traversal</b>	
STUN Server	192.168.2.200
Port Number	3478

The following table describes the labels in this screen.

**Table 50** VoIP > Account 1 (or Account 2) > Server

LABEL	DESCRIPTION
Registrar Server	
Registrar Server	Enter the IP address or domain name of a SIP server. You can use up to 127 printable ASCII characters.
Port Number	Enter the SIP server's listening port number. Keep the default value, if you are not sure of this value.
SIP Service Domain	Enter the IP address or domain name of another SIP server, if your VoIP service provider gave you one. Otherwise, enter the same address that you have entered in the <b>Registrar Server</b> field. You can use up to 64 printable ASCII characters.
Registrar Period Time	Enter the session expiry time in seconds for the phone connections using this account. The allowable range is 60~65535 seconds.  This allows the MAX208M2W Series to automatically disconnect any phone calls using this account after a certain period of inactivity.
Proxy Server	
Proxy Server	Enter the IP address or domain name of the SIP proxy server provided by your VoIP service provider. You can use up to 64 printable ASCII characters.
Port Number	Enter the SIP proxy server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Outbound Server	

**Table 50** VoIP > Account 1 (or Account 2) > Server

LABEL	DESCRIPTION
Outbound Server	Enter the IP address or domain name of the outbound proxy server provided by your VoIP service provider. You can use up to 127 printable ASCII characters. If you choose not to use an outbound proxy server, set this to <b>0.0.0.0</b> .
Port Number	Enter the outbound proxy's listening port number, if your VoIP service provider gave you one. Otherwise, leave it as the default '5060'.  If the outbound proxy is disabled (set to <b>0.0.0.0</b> ), then this port will be ignored.
NAT Traversal	
STUN Server	Enter the IP address or domain name of the STUN server, if your VoIP service provider gave you one. Otherwise, keep the default value.
Port Number	Enter the STUN server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.

## 10.4 Feature

Click **VoIP > Account 1 (or Account 2) > Feature** to configure advanced VoIP features such as DTMF, Call Forwarding, Call Waiting and hotline settings.

**Figure 68** VoIP > Account 1 (or Account 2) > Feature

Feature Settings	
Block Anonymous Call	<input type="checkbox"/>
Do Not Disturb(DND)	<input type="checkbox"/>
Hide User ID	<input type="checkbox"/>
MWI	<input type="checkbox"/>
Hold Method	sendonly/recvonly ▼
DTMF	
DTMF	Out-of-band(RFC 2833) ▼
SIP INFO	<input type="checkbox"/>
Call Forward Setting	
Enable Call Forwarding	<input type="checkbox"/>
Unconditional CF	<input type="checkbox"/>
Unconditional CF Target	0000
Busy CF	<input type="checkbox"/>
Busy CF Target	0000
No Answer CF	<input type="checkbox"/>
No Answer CF Target	0000
Call Waiting Setting	
Call waiting	<input type="checkbox"/>
Hotline Setting	
Hotline	<input type="checkbox"/>
Hotline Target	8888
Hotline Period Time	6 seconds (5-10, default: 6)

The following table describes the labels in this screen.

**Table 51** VoIP > Account 1 (or Account 2) > Feature

LABEL	DESCRIPTION
Feature Settings	
Block Anonymous Call	Select this to have the MAX208M2W Series block all incoming calls from phone that do not send caller ID.
Do Not Disturb (DND)	Select this to have the MAX208M2W Series not forward calls to the phone line.
Hide User ID	Select this to not have your calling number display on the callee's caller ID.
MWI	Select this to enable Message Waiting Indicator (MWI) mode for this phone line. The MAX208M2W Series sends a beeping tone to the phone when there is at least one voicemail for the number.
Hold Method	Select the method to use when a call is put on hold.  <b>sendonly/recvonly</b> - Select this to allow the MAX208M2W Series to send voice packets only but disallow to receive any voice packets. The peer end should change to a state which allows to receive voice packets from the MAX208M2W Series only but disallow to send any voice packets.  <b>inactive</b> - Select this to disallow the MAX208M2W Series send or receive any voice packets.
DTMF	
DTMF	Control how the MAX208M2W Series handles the tones that the phone using this extension makes when you push its buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number.  You should use the same mode as your VoIP service provider. The choices are:  • <b>Out-of-band(RFC 2833)</b> - Follow the RFC 2833 standard and send the DTMF tones in RTP packets.  • <b>In Band</b> - Send the DTMF tones in the voice data stream. This 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	Select this to have the MAX208M2W Series send the DTMF tones in SIP messages.
Call Forward Setting	
Enable call Forwarding	Select this check box to enable call forward.
Unconditional CF, Unconditional CF Target	Select this if you want the MAX208M2W Series to forward all incoming calls to the specified phone number, regardless of other rules in this Call Forward Setting section. Specify the phone number in the <b>Unconditional CF Target</b> field.

**Table 51** VoIP > Account 1 (or Account 2) > Feature

LABEL	DESCRIPTION
Busy CF, Busy CF Target	Select this if you want the MAX208M2W Series to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the <b>Busy CF Target</b> field. 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 CF, No Answer CF Target	Select this if you want the MAX208M2W Series to forward incoming calls to the specified phone number if the call is unanswered. Specify the phone number in the <b>No Answer CF Target</b> field on the right.
Call Waiting Setting	
Call waiting	Select this to enable call waiting for this SIP account on the MAX208M2W Series.
Hotline Setting Configure this section to have the MAX208M2W Series automatically dial the hotline target number after the line is off the hook for the duration specified in the <b>Hotline Period Time</b> field. This is especially useful for dialing emergency numbers.	
Hotline, Hotline Target	Enter the number to be dialed once the MAX208M2W Series has surpassed the delay period.
Hotline Period Time	Enter the duration the phone can remain off the hook before automatically dialing the hotline number. You can set the delay from 5 to 10 seconds.

## 10.5 User

Click **VoIP > Account 1 (or Account 2) > User** to configure advanced VoIP settings such as DTMF, call forwarding, call waiting and hotline settings.

**Figure 69** VoIP > Account 1 (or Account 2) > User

SIP Account	
Enable	<input checked="" type="checkbox"/>
Subscriber Number	<input type="text" value="1000"/>
Display Name	<input type="text" value="1000"/> <small>max length:64 characters</small>
Authentication Name	<input type="text" value="1000"/>
Password	<input type="password" value="****"/>
Codec Settings	
1st Codec	<input type="text" value="G 729"/>
2nd Codec	<input type="text" value="G 711 alaw"/>
3rd Codec	<input type="text" value="G/11 mulaw"/>
Media	
SIP User Agent Name	<input type="text" value="UserAgent"/>
SIP Local Port	<input type="text" value="5060"/> <small>(default:5060)</small>
Session Timer Flag Enable	<input type="checkbox"/>
Session Timer	<input type="text" value="1800"/> <small>seconds (120-65535, default:1800)</small>
Min Session Timer	<input type="text" value="90"/> <small>seconds (90-65535, default:90)</small>
Timeout for Ring back	<input type="text" value="20"/> <small>seconds (1-1000, default:20)</small>

The following table describes the labels in this screen.

**Table 52** VoIP > Account 1 (or Account 2) > User

LABEL	DESCRIPTION
SIP Account	
Enable	Select this if you want the MAX208M2W Series to use this account. Clear it if you do not want the MAX208M2W Series to use this account.
Subscriber 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.
Display Name	Enter the name that appears on the other party's device if they have Caller ID enabled. You can use up to 127 printable ASCII characters.
Authentication Name	Type the SIP user name associated with this account for authentication to the SIP register server.  This field can be 1-31 printable characters (A-Z, a-z, 0-9).
Password	Type the SIP password associated with this account. This field can be 0-31 printable characters (A-Z, a-z, 0-9), underscores (_), pluses (+), periods (.), and "at" symbols (@).
Codec Settings	

**Table 52** VoIP > Account 1 (or Account 2) > User

LABEL	DESCRIPTION
1st Codec, 2nd Codec, 3rd Codec	<p>Select the MAX208M2W Series's first, second, and third choices of the type of voice coder/decoder (codec) that you want the phone line to use when communicating with the SIP server. The following codecs (shown in highest quality to lowest quality order) are supported by the MAX208M2W Series:</p> <ul style="list-style-type: none"> <li>• <b>G.711 aLaw</b> (typically used in Europe)</li> <li>• <b>G.711 muLaw</b> (typically used in North America and Japan)</li> <li>• <b>G.729</b></li> </ul> <p>You can also select <b>NONE</b> for the 2nd and 3rd codecs if your VoIP service provider only gave you one or two codec settings.</p> <p>See <a href="#">Voice Codecs on page 227</a> for more information on voice codecs. When two SIP devices start a SIP session, they must agree on a codec.</p>
Media	
SIP User Agent Name	Enter the name you want to show in the "User-Agent" header of SIP packets sent by this account.
SIP Local Port	Enter the MAX208M2W Series's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Session Timer Flag Enable	Select this activate the MAX208M2W Series's session timer. If you encounter connectivity issues with your network or Internet, then it is suggested that you use the session timer.
Session Timer	<p>Enter the session expiry time in seconds for all phone connections on this trunk The allowable range is 120~65535 seconds. This value cannot be lower than the <b>Min Session Timer</b>.</p> <p>This allows the MAX208M2W Series to automatically disconnect any phone calls on this trunk after a certain period of inactivity.</p>
Min Session Timer	<p>Enter the minimum session expiry time in seconds. The allowable range is 90~65535 seconds.</p> <p>When an incoming call requests a session expiry time that is lower than this, the MAX208M2W Series uses this value instead.</p>
Timeout for Ring back	Enter the maximum number of seconds the MAX208M2W Series has the associated phone ring for an incoming call. After this time period is expired, the MAX208M2W Series has the phone stop ringing. The caller will hear a busy tone then.

## 10.6 Dialing

Click **VoIP > Account 1 (or Account 2) > Dialing** to configure dialing timeout values.

**Figure 70** VoIP > Account 1 (or Account 2) > Dialing

Inter-digit Timeout	<input type="text" value="3"/>	seconds (1~5, default: 3)
First-digit Timeout	<input type="text" value="15"/>	seconds (5~30, default: 15)

The following table describes the labels in this screen.

**Table 53** VoIP > Account 1 (or Account 2) > Dialing

LABEL	DESCRIPTION
Inter-digit Timeout	Enter the maximum number of seconds (1~5) the MAX208M2W Series waits for each digit input of a complete callee number after you press the flash key on the phone. If the MAX208M2W Series cannot receive the next digit entered within this time period, the MAX208M2W Series processes digits you have dialed.
First-digit Timeout	Set the number of seconds (5~30) for the MAX208M2W Series 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.

## 10.7 Speed Dial

Click **VoIP > Account 1 (or Account 2) > Speed Dial** to add, edit, or remove speed-dial rules.

**Figure 71** VoIP > Account 1 (or Account 2) > Speed Dial

**Speed Dial status**

Enable

**Speed Dial Rules**

10 per page    ⏪ ⏩    page ⏪ ⏩

#	Active	Short Number	Real Number	Note
Total Num: 0				

Add    OK

The following table describes the labels in this screen.

**Table 54** VoIP > Account 1 (or Account 2) > Speed Dial

LABEL	DESCRIPTION
Speed Dial Status	
Enable	Select this to enable speed dial on the MAX208M2W Series.
Speed Dial Rules	This is a list of speed dial numbers.



**Table 54** VoIP > Account 1 (or Account 2) > Speed Dial

LABEL	DESCRIPTION
Active	This field displays whether the rule is activated or not.
Short Number	This field displays the speed-dial number you want to use for this phone number.  Select the the speed-dial number you want to use for this phone number if you are editing the entry.
Real Number	This field displays the phone number you want the MAX208M2W Series to call when you use the specified short number.  Enter the phone number you want the MAX208M2W Series to call when you use the specified short number if you are editing the entry.
Notes	This field displays additional information for the speed-dial number.  Enter additional information for the speed-dial number if your are editing the entry.
Remove	Click this to remove the rule.
Add	Click this to add a new speed-dial rule.
OK	Click this to save the changes you made in this table.

## 10.8 FAX

Click **VoIP > Account 1 (or Account 2) > FAX** to configure which standard the account uses for fax services.

**Figure 72** VoIP > Account 1 (or Account 2) > FAX

Options	NONE	▼
---------	------	---

The following table describes the labels in this screen.

**Table 55** VoIP > Account 1 (or Account 2) > FAX

LABEL	DESCRIPTION
Options	<p>Select which standard the MAX208M2W Series uses to handle faxes. The peer devices must also use standard.</p> <p><b>NONE</b> - Disable the fax function.</p> <p><b>G.711A Pass Through</b> - Select this option to send and receive fax messages over the network or Internet using VoIP (G.711a). By encoding fax data as audio data, faxes may be susceptible to packet loss and other errors. However, as this standard is considerably older than T.38, it is more compatible with older orobsolete systems.</p> <p><b>G.711U Pass Through</b> - Select this option to send and receive fax messages over the network or Internet using VoIP (G.711u). By encoding fax data as audio data, faxes may be susceptible to packet loss and other errors. However, as this standard is considerably older than T.38, it is more compatible with older orobsolete systems.</p> <p><b>T.38 FAX Relay</b> - Select this if the MAX208M2W Series should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have interoperability problems.</p>

## 10.9 Technical Reference

The following section contains additional technical information about the MAX208M2W Series features described in this chapter.

### 10.9.1 SIP Call Progression

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

**Table 56** 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.

## 10.9.2 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.



# The VoIP Line Screens

## 11.1 Overview

The **VoIP > Line 1** and **VoIP > Line 2** screens allow you to configure the volume, echo cancellation, VAD settings and custom tones for phone ports 1 and 2 which map to SIP accounts 1 and 2 (see [Chapter 10 on page 139](#)). Since both the **Line 1** and **Line 2** screens are quite similar, this section uses the **VoIP > Line 1** screens to describe the fields.

### 11.1.1 What You Can Do in This Chapter

- The **Phone** screen ([Section 11.2 on page 158](#)) lets you configure phone settings.
- The **Voice** screen ([Section 11.3 on page 159](#)) lets you configure voice settings.
- The **Profile** screen ([Section 11.4 on page 159](#)) lets you configure which country of the world the MAX208M2W Series is in.

### 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 MAX208M2W Series reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

When using VAD, the MAX208M2W Series 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.

## 11.2 Phone

Click **VoIP > Line 1** (or **Line 2**) > **Phone** to configure phone and caller ID settings.

**Figure 73** VoIP > Line 1 (or Line 2) > Phone

Phone	
Hook Flash Detect Upper Bound	<input type="text" value="700"/> msec (100~2000 msec, default:500)
Hook Flash Detect Lower Bound	<input type="text" value="100"/> msec (100~2000 msec, default:80)
Voice Tx Level	<input type="text" value="5"/> ▼
Voice Rx Level	<input type="text" value="5"/> ▼
Caller ID	
Caller ID Type	<input type="text" value="FSK ETSI"/> ▼
Caller ID Display	<input type="text" value="After Ring"/> ▼
Caller ID Power Level	<input type="text" value="0"/> ▼ (default:0)

The following table describes the labels in this screen.

**Table 57** VoIP > Line 1 (or Line 2) > Phone

LABEL	DESCRIPTION
Phone	
Hook Flash Detect Upper Bound	Enter the number of milliseconds for the upper bound of a quick on-hook and off-hook cycle in order to recognize a hook flash event.
Hook Flash Detect Lower Bound	Enter the number of milliseconds for the lower bound of a quick on-hook and off-hook cycle in order to recognize a hook flash event.
Voice Tx Level	Select the volume level transmitted by the MAX208M2W Series. -9 is the quietest, and 9 is the loudest.
Voice Rx Level	Select the volume level transmitted to the MAX208M2W Series. -9 is the quietest, and 9 is the loudest.
Caller ID	
Caller ID Type	Select the caller ID type ( <b>FSK Bellcore</b> , <b>Japan CLIP</b> , or <b>FSK ETSI</b> ) for the region in which the MAX208M2W Series is located. You can also <b>Disable</b> caller ID (means to not display the remote caller ID on the phone).
Caller ID Display	Select when to display the caller ID of incoming calls on the associated phone, before or after it rings ( <b>Before Ring</b> or <b>After Ring</b> ).
Caller ID Power Level	Enter the transmitting power level (0~3) the MAX208M2W Series uses to display caller ID on the associated phone. The corresponding power for each number: <ul style="list-style-type: none"> <li>0: -13.5 dBm</li> <li>1: -13 dBm</li> <li>2: -12 dBm</li> <li>3: -11 dBm</li> </ul>

## 11.3 Voice

Click **VoIP > Line 1 (or Line 2) > Voice** to configure voice settings.

**Figure 74** VoIP > Line 1 (or Line 2) > Voice

<b>VAD</b>	
Voice Active Detector	Disable <input type="button" value="v"/> default: disable
<b>LEC</b>	
Line Echo Canceller Tail Length	48 msec. <input type="button" value="v"/> default: 48 ms

The following table describes the labels in this screen.

**Table 58** VoIP > Line 1 (or Line 2) > Voice

LABEL	DESCRIPTION
VAD - Voice Activity Detection	
Voice Active Detector	Select one of the following <b>Silence Suppression</b> option to have the MAX208M2W Series stop transmitting voice traffic when you are not speaking using the detection method. This reduces the bandwidth the MAX208M2W Series uses. <ul style="list-style-type: none"> <li>• <b>Silence Suppression - NO CNG</b></li> <li>• <b>Silence Suppression - Only G.711 AnnexII Type</b></li> <li>• <b>Silence Suppression - Codec Specific CN</b></li> </ul> Select <b>Disable</b> to turn this feature off.
LEC - Line Echo Cancellation	
Line Echo Canceller Tail Length	Select the maximum number of milliseconds of an echo length (16 ms, 32 ms or 48 ms) the MAX208M2W Series can handle and eliminate the effect. An echo is normally caused by the sound of your voice reverberating in the telephone receiver while you talk. Select Disable  Question: How if an echo's length is longer than the set value?

## 11.4 Profile

Click **VoIP > Line 1 (or Line 2) > Profile** to maintain settings that depend on which region of the world the MAX208M2W Series is in.

**Figure 75** VoIP > Line 1 (or Line 2) > Profile

<b>Country Profile</b>	
Country Profile	Default <input type="button" value="v"/>

The following table describes the labels in this screen.

**Table 59** VoIP > Line 1 (or Line 2) > Profile

LABEL	DESCRIPTION
Country Profile	Select the place in which the MAX208M2W Series is located, <b>USA</b> or any other country ( <b>Default</b> ).



# Maintenance

## 12.1 Overview

Use these screens to manage and maintain your MAX208M2W Series.

### 12.1.1 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 You have disabled that service in one of the remote management screens.
- 2 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the MAX208M2W Series will disconnect the session immediately.
- 3 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 MAX208M2W Series's WAN IP address when configuring from the WAN.
- Use the MAX208M2W Series's LAN IP address when configuring from the LAN.

## System Timeout

There is a default system management idle timeout of five minutes. The MAX208M2W Series 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 MAX208M2W Series supports SNMP agent functionality, which allows a manager station to manage and monitor the MAX208M2W Series through the network. The MAX208M2W Series supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

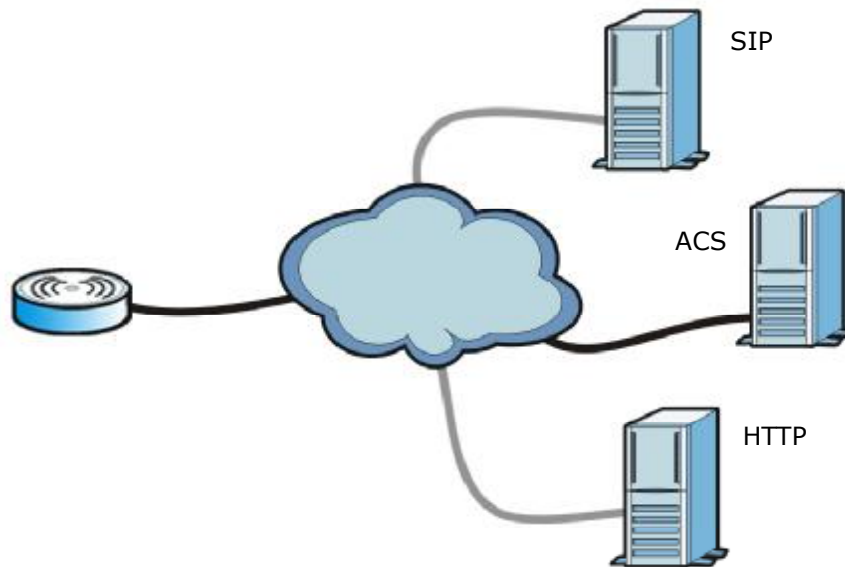
Note: SNMP is only available if TCP/IP is configured.

**TR-069**

TR-069 is an abbreviation of “Technical Reference 069”, a protocol designed to facilitate the remote management of Customer Premise Equipment (CPE), such as the MAX208M2W Series. It can be managed over a WAN by means of an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between the ACS and the client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the MAX208M2W Series, modify its settings, perform firmware upgrades, and monitor and diagnose it. In order to do so, you must enable the TR-069 feature on your MAX208M2W Series and then configure it appropriately. (The ACS server which it will use must also be configured by its administrator.)

**Figure 76** TR-069 Example



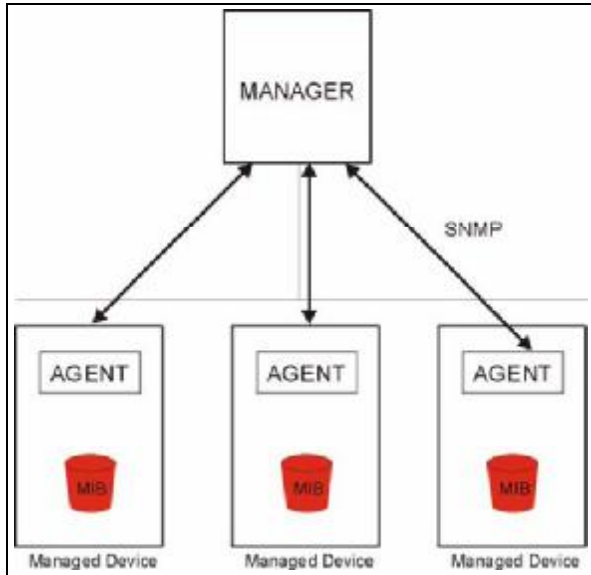
In this example, the MAX208M2W Series receives data from at least 3 sources: A SIP server for handling voice calls, an HTTP server for handling web services, and an ACS, for configuring the MAX208M2W Series remotely. All three servers are owned and operated by the client’s Internet Service Provider. However, without the configuration settings from the ACS, the MAX208M2W Series cannot access the other two servers. Once the MAX208M2W Series receives its configuration settings and implements them, it can connect to the other servers. If the settings change, it will once again be unable to connect until it receives its updates from the ACS.

The MAX208M2W Series can be configured to periodically check for updates from the auto-configuration server so that the end user need not be worried about it.

## SNMP

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

**Figure 77** SNMP Management Model



An agent is a management software module that resides in a managed device (the MAX208M2W Series). 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 MAX208M2W Series 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.

The MAX208M2W Series sends traps to the SNMP manager when any of the following events occurs:

**Table 60** 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, CI 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.

## OMA-DM

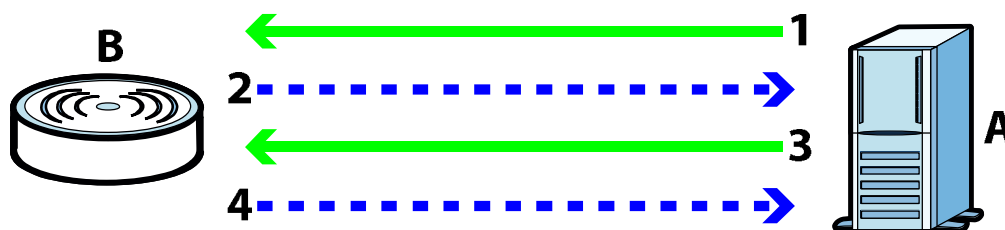
When the MAX208M2W Series initiates communication with the server (often times at start up or after the first time you turn it on), the server uploads commands, new files (if any), and other information used by a service provider to customize the MAX208M2W Series's features.

Device management works as follows:

- 1 The server (**A**) sends out the query (**1**) to the MAX208M2W Series (**B**).
- 2 The MAX208M2W Series responds by sending back its credentials (**2**), to which the server responds with its credentials along with a string of management operations (**3**).
- 3 The client responds to the management operations (**4**), perhaps confirming file alterations or confirming receipt of file uploads and so on.

- 4 The server disconnects from the MAX208M2W Series once all of its management operations have been carried out.

**Figure 78** OMA-DM Data Management



### OMA-DM Authentication

In order to ensure the integrity of the connection between an OMA-DM server and the MAX208M2W Series, communication between the two is encoded using one of three common algorithms. They are not intended to be used in lieu of proper digital security, but instead as a means of transmitting multiple disparate types of data over HTTP. Security encryption for communication is handled by different processes configured elsewhere in the MAX208M2W Series's web configurator

**Basic Access Authentication** – Sends a person's user name and password in Base64. This authentication protocol is supported by all browsers that are HTTP 1.0/1.1 compliant. Although converted to Base64 for the sake of cross-compatibility, credentials are nonetheless passed between the web browser and the server in plaintext, making it extremely easy to intercept and read. As such, it is rarely used anymore.

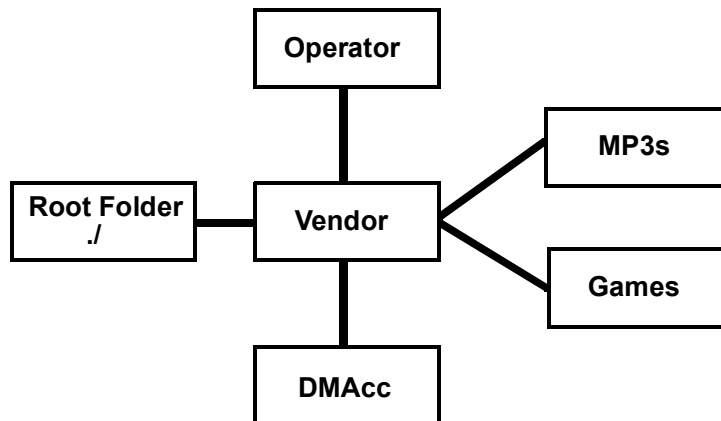
**Digest Access Authentication** – This protocol was designed to replace basic access authentication. Instead of encoding a user name and password in plaintext, this protocol uses what is known as an MD5 message authentication code. It allows the server to issue a single-use, randomly generated number (known as a 'nonce') to the client (in this case, the web browser), which then uses the number as the 'public key' for encrypting its data. When the server receives the encrypted data, it unlocks it using the 'key' that was just provided. While stronger than basic access authentication, this protocol is not as strong as, say, HMAC, or as secure as the client using a client-side private key encryption scheme.

**Hash Message Authentication Code** – Also known as HMAC, this code relies on cryptographic hash functions to bolster an existing protocol, such as MD5. It is a method for generating a stronger, significantly higher encryption key.

## OMA-DM Data Model

Each device that conforms to the current OMA-DM standard has an identical data structure embedded in its controlling firmware. This allows a similarly conforming OMA-DM server to navigate the folder structure and to make file alterations where appropriate or required.

**Figure 79** OMA-DM Data Model



In the example data model shown here, the parent folders must conform to the OMA-DM standard. The child folders, on the other hand, can be customized on an individual basis. This allows the parent folders to all maintain a consistent URI (Uniform Resource Identifier) across all devices that meet the OMA-DM standard's requirements.

For example, in the preceding figure the URI for the "Games" folder is `"/Vendor/Games/"`. The `"/Vendor/"` portion of the URI exists on all devices that conform to the OMA-DM standard. The "Games" folder, however, may or may not exist depending on the services provided by the company managing the device.

## 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.

## 12.2 Password

Use this screen to set up admin and guest accounts for logging into and managing the WiMAX Device. The "admin" user can access and configure all screens. The "guest" user can only perform some basic settings such as viewing the system status information, configuring LAN, NAT, DDNS, and Firewall settings and reset the MAX208M2W Series to factory defaults and restart the MAX208M2W Series.

Click **Maintenance > Password** to open this screen as shown next.

**Figure 80** Password Screen

The screenshot shows a web form titled "Change Password". It contains the following elements:

- Group:** A dropdown menu with "admin" selected.
- Old Password:** A text input field.
- New Password:** A text input field.
- Retype:** A text input field.

This screen contains the following fields:

**Table 61** Password

LABEL	DESCRIPTION
Group	Select the group for which you want to change the login password.
Old Password	Enter the old password for the login group.
New Password	Enter the new password for the login group.
Retype	Retype the new password for the login group.



## 12.3 HTTP

Use this screen to allow remote access to the WiMAX Device from a network connection over HTTP.

Click **Maintenance > Remote MGMT > HTTP** to open this screen as shown next.

**Figure 81** HTTP Screen

<b>HTTP Server</b>	
Enable	<input checked="" type="checkbox"/>
Port Number	<input type="text" value="80"/>
<b>HTTPS Server</b>	
Enable	<input checked="" type="checkbox"/>
Port Number	<input type="text" value="443"/>
<b>HTTP and HTTPS</b>	
Allow Connection from WAN	<input checked="" type="checkbox"/>
<b>HTTP Session Timeout</b>	
Session Timeout	<input type="text" value="5"/> minutes (0-99, default:5, 0 means disabled)

This screen contains the following fields:

**Table 62** HTTP

LABEL	DESCRIPTION
HTTP Server	
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the MAX208M2W Series. The computer must use the same port number.
HTTPS Server	
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the MAX208M2W Series. The computer must use the same port number.
HTTP and HTTPS	
Allow Connection from WAN	Select this to allow incoming connections from the WAN over either HTTP or HTTPS.
HTTP Session Timeout	
Session Timeout	Enter the number of minutes (0-99) the MAX208M2W Series waits to delete an inactive web connection (HTTP or HTTPS).

## 12.4 Telnet

Use this screen to allow remote access to the WiMAX Device from a network connection over Telnet.

Click **Maintenance > Remote MGMT > Telnet** to open this screen as shown next.

**Figure 82** Telnet Screen

Enable	<input checked="" type="checkbox"/>
Port Number	<input type="text" value="23"/>
Allow Connection from WAN	<input checked="" type="checkbox"/>
Allow Connection from LAN	<input checked="" type="checkbox"/>

This screen contains the following fields:

**Table 63** Telnet

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the MAX208M2W Series. The computer must use the same port number.
Allow Connection from WAN	Select this to allow connections using this service that originate on the WAN.
Allow Connection from LAN	Select this to allow connection using this service that originate on the LAN.

## 12.5 SSH

Use this screen to allow remote access to the WiMAX Device from a network connection over SSH.

Click **Maintenance > Remote MGMT > SSH** to open this screen as shown next.

**Figure 83** SSH Screen

Enable	<input checked="" type="checkbox"/>
Port Number	<input type="text" value="22"/>
Allow Connection from WAN	<input checked="" type="checkbox"/>
Allow Connection from LAN	<input checked="" type="checkbox"/>

This screen contains the following fields:

**Table 64** SSH

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the MAX208M2W Series. The computer must use the same port number.
Allow Connection from WAN	Select this to allow connections using this service that originate on the WAN.
Allow Connection from LAN	Select this to allow connection using this service that originate on the LAN.

## 12.6 SNMP

Use this screen to allow remote access to the WiMAX Device from a network connection over SNMP.

Click **Maintenance > Remote MGMT > SNMP** to open this screen as shown next.

**Figure 84** SNMP Screen

Enable	<input type="checkbox"/>
Location	<input type="text"/>
Contact	<input type="text"/>
Read Community	<input type="text" value="public"/>
Write Community	<input type="text" value="private"/>
Trap Server	<input type="text" value="192.168.0.1"/>
Trap Community	<input type="text" value="test"/>

This screen contains the following fields:

**Table 65** SNMP

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Location	Enter the location of the SNMP server (for example, "Engineering Dept., Floor 6, Building A, New York City").
Contact	Enter contact information for the administrator managing the SNMP server (for example, "Bill Smith, IT Dept., (555) 555-5454").
Read Community	Enter the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Write Community	Enter the password for incoming Set requests from the management station. The default is public and allows all requests.

**Table 65** SNMP (continued)

LABEL	DESCRIPTION
Trap Server	Enter the IP address of the station to send your SNMP traps to.
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.

## 12.7 CWMP

Use this screen to allow CWMP connections for remote management, firmware upgrades and troubleshooting.

Click **Maintenance > Remote MGMT > CWMP** to open this screen as shown next.

**Figure 85** CWMP Screen

Enable	<input type="checkbox"/>
ACS Server URL	<input type="text"/>
Bootstrap Enable	<input checked="" type="checkbox"/>
ACS Username	<input type="text"/>
ACS Password	<input type="text"/>
Periodical Inform Enable	<input checked="" type="checkbox"/>
Periodical Inform Interval	<input type="text" value="30"/>
Connection Request Username	<input type="text"/>
Connection Request Password	<input type="text"/>
CA Certificate File	<input type="text"/> Browse...
CA Certificate Info	<input type="text" value="/C=TW/ST=testST/L=testL/O=testO/CN=testCA"/>
Client Certificate File	<input type="text"/> Browse...
Client Certificate Info	<input type="text" value="/C=TW/ST=testST/L=testL/O=testO/CN=testClient"/>

This screen contains the following fields:

**Table 66** CWMP

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
ACS Server URL	Enter the URL or IP address of the auto-configuration server.
Bootstrap Enable	Select this to enable bootstrap events.
ACS Username	Enter the user name sent when the MAX208M2W Series connects to the ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.

**Table 66** CWMP (continued)

LABEL	DESCRIPTION
ACS Password	Enter the password sent when the MAX208M2W Series connects to an ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.
Periodical Inform Enable	Select this to allow the MAX208M2W Series to periodically connect to the ACS and check for configuration updates.  If you do not enable this feature then the MAX208M2W Series can only be updated automatically when the ACS initiates contact with it and if you selected the checkbox on this screen.
Periodical Inform Interval	Enter the time interval (in seconds) at which the MAX208M2W Series connects to the auto-configuration server.
Connection Request Username	Enter the connection request user name that the ACS must send to the MAX208M2W Series when it requests a connection.  You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.  <b>Note:</b> This must be provided by the ACS administrator.
Connection Request Password	Enter the connection request password that the ACS must send to the MAX208M2W Series when it requests a connection.  You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.  <b>Note:</b> This must be provided by the ACS administrator.
CA Certificate File	Click <b>Browse</b> to upload a Certificate Authority (CA) certificate to the MAX208M2W Series.
CA Certificate Info	This displays information about the currently active CA certificate.
Client Certificate File	Click <b>Browse</b> to upload a client certificate to the MAX208M2W Series.
Client Certificate Info	This displays information about the currently active client certificate.

## 12.8 OMA-DM

Use this screen to allow remote access to the WiMAX Device from a network connection over OMA-DM.

Click **Maintenance > Remote MGMT > OMA-DM** to open this screen as shown next.

**Figure 86** OMA-DM Screen

Enable	<input type="checkbox"/>
Server URL	<input type="text"/>
Server Port	80
Server Auth Type	NONE
Server ID	<input type="text"/>
Server Password	<input type="text"/>
Server Nonce	<input type="text"/>
Client Auth Type	NONE
Client ID	<input type="text"/>
Client Password	<input type="text"/>
Client Nonce	<input type="text"/>
Periodical Client-initiated Enable	<input checked="" type="checkbox"/>
Periodical Client initiated Interval	3600 seconds (default 3600)

This screen contains the following fields:

**Table 67** OMA-DM

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Server URL	Enter the IP address or URL of the OMA-DM server that you intend to use to manage this device.
Server Port	Enter the port number for the IP address of the OMA-DM server set up in the preceding field.
Server Auth Type	Select the encryption algorithm scheme used by the OMA-DM server to communicate with client devices. If the scheme selected here does not match the actual scheme used by the server, then server will challenge the MAX208M2W Series to automatically update its settings. <ul style="list-style-type: none"> <li>• <b>None</b> - No authentication.</li> <li>• <b>Basic</b> - Server ID and Password are encoded using a Basic Access Authentication Code.</li> <li>• <b>Digest (MD5)</b> - Server ID and Password are encoded using a Digest Access Authentication Code.</li> <li>• <b>HMAC</b> - Server ID and Password are encoded using a keyed Hash Message Authentication Code.</li> </ul>
Server ID	Enter the identification code for the server. This is used by the MAX208M2W Series during the communication handshake process to identify the server.

**Table 67** OMA-DM (continued)

LABEL	DESCRIPTION
Server Password	Enter the password for the server's identification code. This shared public key is used by the MAX208M2W Series during the communication handshake process to identify the server.
Server Nonce	<p>The MAX208M2W Series and the OMA-DM server use nonces to authenticate each other if you select <b>MD5</b> as the authentication algorithm in the <b>Server Auth Type</b> field. Nonce is an abbreviation of 'number used once'. It is normally a random or pseudo-random number applied in an authentication protocol to protect existing communications from being reused in 'replay attacks'.</p> <p>Type up to 20 digits for the OMA-DM server nonce.</p>
Client Auth Type	<p>Select the encryption algorithm scheme used by the OMA-DM server to communicate with client devices. If the scheme selected here does not match the actual scheme used by the server, then server will challenge the MAX208M2W Series to automatically update its settings.</p> <ul style="list-style-type: none"> <li>• <b>None</b> - No authentication.</li> <li>• <b>Basic</b> - Server ID and Password are encoded using a Basic Access Authentication Code.</li> <li>• <b>Digest (MD5)</b> - Server ID and Password are encoded using a Digest Access Authentication Code.</li> <li>• <b>HMAC</b> - Server ID and Password are encoded using a keyed Hash Message Authentication Code.</li> </ul> <p><b>Note:</b> Make sure that the scheme selected here matches the the <b>Server Auth Type</b>.</p>
Client ID	Enter the client name for the MAX208M2W Series.
Client Password	Enter the password for the MAX208M2W Series's client name.
Client Nonce	<p>The MAX208M2W Series and the OMA-DM server use nonces to authenticate each other if you select <b>MD5</b> as the authentication algorithm in the <b>Client Auth Type</b> field.</p> <p>Type up to 20 digits for the OMA-DM client nonce.</p>
Periodical Client-Initiated Enable	<p>Select this to allow the MAX208M2W Series to periodically connect to the OMA-DM server and check for configuration updates.</p> <p>If you do not enable this feature then the MAX208M2W Series can only be updated automatically when the OM-DM server initiates contact with it and if you selected the checkbox on this screen.</p>
Periodical Client-Initiated Interval	Enter the time interval (in seconds) at which the MAX208M2W Series connects to the OMA-DM server.

## 12.9 Date

Use these settings to set the system time or configure an NTP server for automatic time synchronization.

Click **Maintenance > Date/Time > Date** to open this screen as shown next.

**Figure 87** Date Screen

Current System Time	Tue Jan 13 13:21:04 1970		
<input type="radio"/> Manual			
New Time(hh:mm:ss)	15	: 42	: 02
New Date(mm-dd-yyyy)	07	- 26	- 2010
<input checked="" type="radio"/> Get from Time Server			
Time Protocol	NTP (RFC-1305) ▼		
Time Server Address 1	1.my.pool.ntp.org		
Time Server Address 2	2.my.pool.ntp.org		
Time Server Address 3	3.my.pool.ntp.org		
Time Server Address 4	4.my.pool.ntp.org		

This screen contains the following fields:

**Table 68** Date

LABEL	DESCRIPTION
Manual	
New Time	Enter the new time in this field.
New Date	Enter the new date in this field.
Get from Time Server	
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. <ul style="list-style-type: none"> <li>• <b>NTP (RFC 1305)</b> - This format is similar to Time (RFC 868).</li> </ul>
Time Server Address 1~4	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.



## 12.10 Time Zone

Use this screen to set the time zone in which the WiMAX device is physically located.

Click **Maintenance > Date/Time > Time Zone** to open this screen as shown next.

**Figure 88** Time Zone Screen

Time Zone	(GMT+08:00) Kuala Lumpur, Singapore				
Enable Daylight Saving	<input type="checkbox"/>				
Start Date	First	Sunday	of	April	at 2 o'clock
End Date	Last	Sunday	of	October	at 2 o'clock

This screen contains the following fields:

**Table 69** Time Zone

LABEL	DESCRIPTION
Time Zone	Select the time zone at your location.
Enable Daylight Savings Time	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.

## 12.11 Upgrade File

Use this screen to browse to a firmware file on a local computer and upload it to the WiMAX Device. Firmware files usually use the system model name with a "\*.bin" extension, such as "MAX208M2W Series.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system restarts.

Contact your service provider for information on available firmware upgrades.

Note: Only use firmware for your MAX208M2W Series's specific model.

Click **Maintenance > Firmware Upgrade > Upgrade File** to open this screen as shown next.

**Figure 89** Upgrade File Screen



This screen contains the following fields:

**Table 70** Upgrade File

LABEL	DESCRIPTION
Upgrade File	Click <b>Browse</b> then browse to the location of a firmware upgrade file and select it.
Upgrade	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!

### 12.11.1 The Firmware Upload Process

When the MAX208M2W Series 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.

## 12.12 Upgrade Link

Use this screen to set the URL of a firmware file on a remote computer and upload it to the WiMAX Device.

Click **Maintenance > Firmware Upgrade > Upgrade Link** to open this screen as shown next.

**Figure 90** Upgrade Link Screen

The screenshot shows a rectangular window with a title bar. Inside, the text 'Upgrade Link' is positioned to the left of a horizontal text input field. Below the input field, centered, is a button labeled 'Upgrade'.

This screen contains the following fields:

**Table 71** Upgrade Link

LABEL	DESCRIPTION
Upgrade Link	Enter the URL or IP address of the firmware's upgrade location on the network.
Upgrade	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!

## 12.13 CWMP Upgrade

Use this screen to upgrade the firmware on the WiMAX Device using CWMP Request Download.

Click **Maintenance > Firmware Upgrade > CWMP Upgrade** to open this screen as shown next.

**Figure 91** CWMP Upgrade Screen

The screenshot shows a rectangular window with a title bar. Inside, the text 'Upgrade Firmware via CWMP Request Download' is positioned at the top left. Below this text, centered, is a button labeled 'Upgrade'.

This screen contains the following fields:

**Table 72** CWMP Upgrade

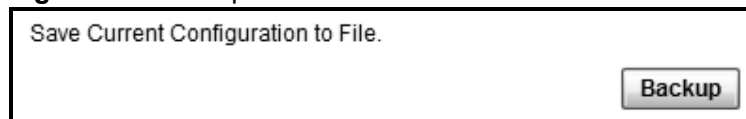
LABEL	DESCRIPTION
Upgrade	Click this to begin upgrading firmware using CWMP Request. This may take up to two minutes.  Note: Do not turn off the device while firmware upload is in progress!

## 12.14 Backup

Use this screen to backup your current WiMAX Device settings to a local computer.

Click **Maintenance > Backup/Restore > Backup** to open this screen as shown next.

**Figure 92** Backup/Restore Screen



This screen contains the following fields:

**Table 73** Backup/Restore

LABEL	DESCRIPTION
Backup	Click this to save the MAX208M2W Series'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.

## 12.15 Restore

Use this screen to restore your WiMAX Device settings from a backup file on a local computer.

Click **Maintenance > Backup/Restore > Restore** to open this screen as shown next.

**Figure 93** Restore Screen

This screen contains the following fields:

**Table 74** Restore

LABEL	DESCRIPTION
Configuration File	Click <b>Choose File</b> then browse to the location of a firmware upgrade file and select it.  Click <b>File Restore</b> to upload the specified configuration to the MAX208M2W Series and replace the current settings.
Backup Configuration File URL	Enter the URL or IP address of the backup configuration file's location on the network.  Click <b>URL Restore</b> to upload the specified configuration to the MAX208M2W Series and replace the current settings.

### 12.15.1 The Restore Configuration Process

When the MAX208M2W Series 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 MAX208M2W Series'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.

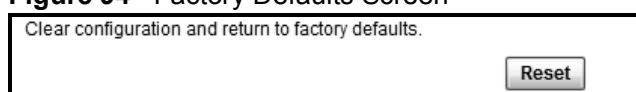
If the upload was not successful, you are notified with an error message.

## 12.16 Factory Defaults

Use this screen to restore the WiMAX Device to its factory default settings.

Click **Maintenance > Backup/Restore > Factory Defaults** to open this screen as shown next.

**Figure 94** Factory Defaults Screen



Clear configuration and return to factory defaults.

Reset

This screen contains the following fields:

**Table 75** Factory Defaults

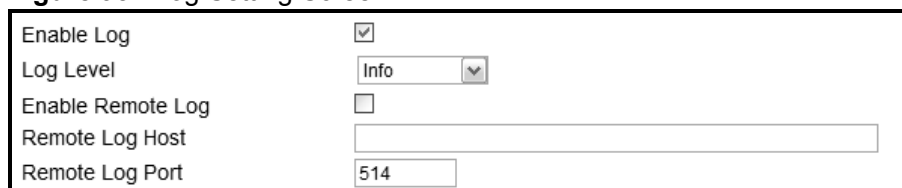
LABEL	DESCRIPTION
Reset	Click this to clear all user-entered configuration information and return the MAX208M2W Series to its factory defaults. There is no warning screen.

## 12.17 Log Setting

Use this screen to configure which type of events on the WiMAX Device are logged.

Click **Maintenance > LOG > Log Setting** to open this screen as shown next.

**Figure 95** Log Setting Screen



Enable Log

Log Level

Enable Remote Log

Remote Log Host

Remote Log Port

This screen contains the following fields:

**Table 76** Log Setting

LABEL	DESCRIPTION
Enable Log	Select this to have the MAX208M2W Series log network activity according to the selected <b>Log Level</b> .
Log Level	Select the type of logs to record.

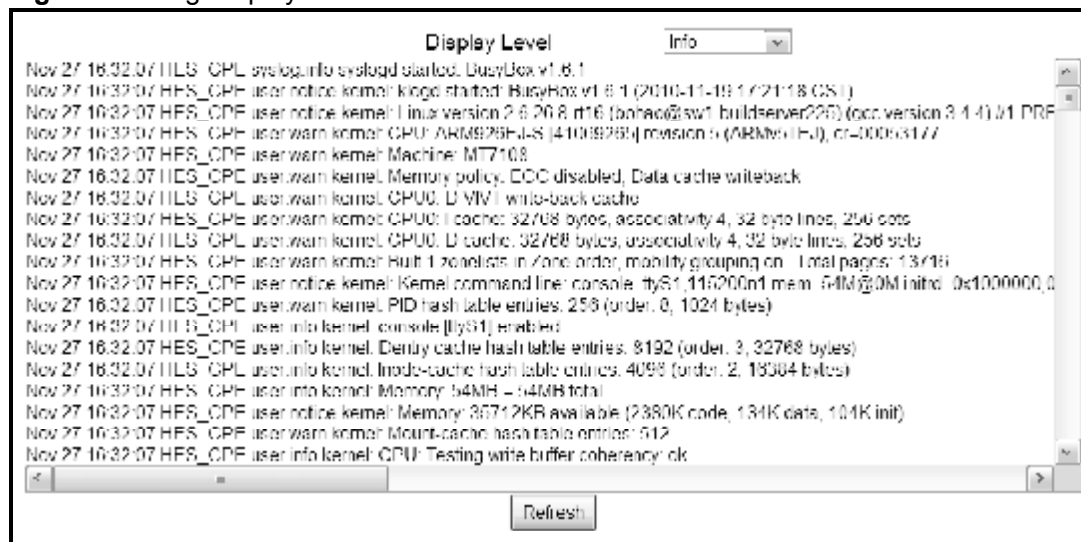
**Table 76** Log Setting (continued)

LABEL	DESCRIPTION
Enable Remote Log	Select this to allow logs to be recorded and stored on a remote logs server.
Remote Log Host	Enter the remote log host IP address if <b>Enable Remote Log</b> is selected.
Remote Log Port	Enter the remote log host port if <b>Enable Remote Log</b> is selected.

## 12.18 Log Display

Use this screen to view the log messages of the WiMAX Device.

Click **Maintenance > LOG > Log Display** to open this screen as shown next.

**Figure 96** Log Display Screen

This screen contains the following fields:

**Table 77** Log Display

LABEL	DESCRIPTION
Display Level	Select the type of logs to display from this menu.
Refresh	Click this to refresh the logs in the display window.

## 12.19 Ping Test

Use this screen to test network connectivity using ping.

Click **Maintenance > Network Test > Ping** to open this screen as shown next.

**Figure 97** Ping Screen

This screen contains the following fields:

**Table 78** Ping

LABEL	DESCRIPTION
IP Address	Enter the IP address or domain name of a target device to which this test will send.
Ping	Click this to start the test. The result will show at the bottom of the screen.

## 12.20 Traceroute Test

Use this screen to test network connectivity using traceroute.

Click **Maintenance > Network Test > Traceroute** to open this screen as shown next.

**Figure 98** Traceroute Screen

This screen contains the following fields:

**Table 79** Traceroute

LABEL	DESCRIPTION
IP Address	Enter the IP address or domain name of a target device to which this test will send.
Traceroute	Click this to start the test. The result will show at the bottom of the screen.

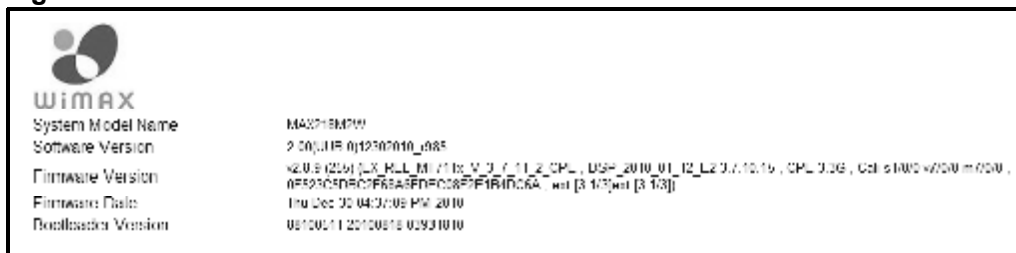


## 12.21 About

This screen displays information about the MAX208M2W Series that can be useful when upgrading firmware, considering deployment options, and working with technical support if the device encounters difficulties.

Click **Maintenance > About** to open this screen as shown next.

**Figure 99** About Screen



This screen contains the following fields:

**Table 80** About

LABEL	DESCRIPTION
System Model Name	This field displays the MAX208M2W Series system name. It is used for identification.
Software Version	This field displays the Web Configurator software version that the MAX208M2W Series is currently running.
Firmware Version	This field displays the current version of the firmware inside the device.
Firmware Date	This field displays the date the firmware version was created.
Bootloader Version	This field displays the bootloader version.

## 12.22 Reboot

Use this screen to perform a software restart of the WiMAX Device. You may log in again within a few minutes of using the reboot button.

Click **Maintenance > Reboot** to open this screen as shown next.

**Figure 100** Reboot Screen



This screen contains the following fields:

**Table 81** Reboot

LABEL	DESCRIPTION
Reboot	Click this button to have the device perform a software restart. The <b>Power</b> LED blinks as it restarts and the shines steadily if the restart is successful.  Note: Wait one minute before logging back into the MAX208M2W Series after a restart.

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories:

- [Power, Hardware Connections, and LEDs](#)
- [MAX208M2W Series Access and Login](#)
- [Internet Access](#)
- [Reset the MAX208M2W Series to Its Factory Defaults](#)

## 13.1 Power, Hardware Connections, and LEDs

---

The MAX208M2W Series does not turn on. None of the LEDs turn on.

---

- 1 Make sure you are using the power adapter or cord included with the MAX208M2W Series.
- 2 Make sure the power adapter or cord is connected to the MAX208M2W Series and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adapter or cord to the MAX208M2W Series.
- 4 If the problem continues, contact the vendor.

---

One of the LEDs does not behave as expected.

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.2.1 on page 21](#) for more information.
- 2 Check the hardware connections. See the Quick Start Guide.

- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adapter to the MAX208M2W Series.
- 5 If the problem continues, contact the vendor.

## 13.2 MAX208M2W Series Access and Login

---

I forgot the IP address for the MAX208M2W Series.

---

- 1 The default IP address is .
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the MAX208M2W Series by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the MAX208M2W Series (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the MAX208M2W Series to its factory defaults. See [Section 12.16 on page 182](#).

I forgot the password.

---

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the MAX208M2W Series to its factory defaults. See [Section 12.16 on page 182](#).

I cannot see or access the **Login** screen in the web configurator.

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is .
  - If you changed the IP address ([Section 7.6 on page 99](#)), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the MAX208M2W Series](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.2.1 on page 21](#).
  - 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Appendix C on page 237](#).
  - 4 If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. Your MAX208M2W Series is a DHCP server by default.  
If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the MAX208M2W Series. See [Appendix D on page 247](#).
  - 5 Reset the MAX208M2W Series to its factory defaults, and try to access the MAX208M2W Series with the default IP address. See [Chapter 2 on page 25](#).
  - 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Try to access the MAX208M2W Series using another service, such as Telnet. If you can access the MAX208M2W Series, check the remote management settings and firewall rules to find out why the MAX208M2W Series does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

---

[I can see the Login screen, but I cannot log in to the MAX208M2W Series.](#)

---

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the MAX208M2W Series. Log out of the MAX208M2W Series in the other session, or ask the person who is logged in to log out.
- 3 Disconnect and re-connect the power adapter or cord to the MAX208M2W Series.
- 4 If this does not work, you have to reset the MAX208M2W Series to its factory defaults. See [Section 12.16 on page 182](#).

---

### I cannot Telnet to the MAX208M2W Series.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

## 13.3 Internet Access

---

### I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.2.1 on page 21](#).
- 2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 Check your security settings. See [Chapter 8 on page 127](#).
- 4 Check your WiMAX settings. The MAX208M2W Series may have been set to search the wrong frequencies for a wireless connection. See [Chapter 6 on page 69](#). If you are unsure of the correct values, contact your service provider.
- 5 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 6 Disconnect all the cables from your MAX208M2W Series, and follow the directions in the Quick Start Guide again.
- 7 If the problem continues, contact your ISP.

---

### I cannot access the Internet any more. I had access to the Internet (with the MAX208M2W Series), but my Internet connection is not available any more.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.2.1 on page 21](#).
- 2 Disconnect and re-connect the power adapter to the MAX208M2W Series.

- 3 If the problem continues, contact your ISP.

---

#### The Internet connection is slow or intermittent.

---

- 1 The quality of the MAX208M2W Series's wireless connection to the base station may be poor. Poor signal reception may be improved by moving the MAX208M2W Series away from thick walls and other obstructions, or to a higher floor in your building.
- 2 There may be radio interference caused by nearby electrical devices such as microwave ovens and radio transmitters. Move the MAX208M2W Series away or switch the other devices off. Weather conditions may also affect signal quality.
- 3 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.2.1 on page 21](#). If the MAX208M2W Series is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 4 Disconnect and re-connect the power adapter to the MAX208M2W Series.
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

---

#### The Internet connection disconnects.

---

- 1 Check your WiMAX link and signal strength using the **Strength Indicator** LEDs on the device.
- 2 Contact your ISP if the problem persists.

## 13.4 Reset the MAX208M2W Series to Its Factory Defaults

If you reset the MAX208M2W Series, you lose all of the changes you have made. The MAX208M2W Series re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

---

You will lose all of your changes when you push the **Reset** button.

---

To reset the MAX208M2W Series,

- 1 Make sure the **Power LED** is on and not blinking.
- 2 Press and hold the **Reset** button for five to ten seconds. Release the **Reset** button when the **Power** LED begins to blink. The default settings have been restored.

If the MAX208M2W Series restarts automatically, wait for the MAX208M2W Series to finish restarting, and log in to the web configurator. The password is "1234".

If the MAX208M2W Series does not restart automatically, disconnect and reconnect the MAX208M2W Series's power. Then, follow the directions above again.

### 13.4.1 Pop-up Windows, JavaScript and Java Permissions

Please see [Appendix C on page 237](#).



# Product Specifications

This chapter gives details about your MAX208M2W Series's hardware and firmware features.

**Table 82** Environmental and Hardware Specifications

FEATURE	DESCRIPTION
Operating Temperature	0°C to 45°C
Storage Temperature	-25°C to 55°C
Operating Humidity	10% ~ 95% (non-condensing)
Storage Humidity	10% to 95% (non-condensing)
Power Supply	12V DC, 2A
Power consumption	24 Watts maximum
Ethernet Interface	Two auto-negotiating, auto-MDI/MDI-X NWay 10/100 Mbps RJ-45 Ethernet ports
Telephony Interface	Two analog ATA interfaces for standard telephones through RJ-11 FXS (Foreign Exchange Subscriber) analog connector
Antennas	Two 6 +/- 0.5dBi Omni directional antennas
Weight	493g
Dimensions	259 mm (W) x 93 mm (D) x 164 mm (H)
Certification	<ul style="list-style-type: none"> <li>• FCC - MAX208M2W; CE - MAX218M2W</li> <li>• Comply with WiMAX Forum Wave II standard.</li> <li>• WEEE Eco directive 2002/95/EC. Full RoHS (6/6)</li> <li>• 2002/96/EC (WEEE) (WEEE) Waste Electrical and Electronic Equipment Directive</li> <li>• EEE (Proposal for Directive on Environmental Impacts of Electrical and Electronic Equipment).</li> <li>• Reach Compliance</li> <li>• EMC <ul style="list-style-type: none"> <li>◦ EN 301 489-1 and EN 301 489-17. Emission class B.</li> </ul> </li> <li>• RF ETSI <ul style="list-style-type: none"> <li>◦ EN 302 326</li> </ul> </li> <li>• Safety <ul style="list-style-type: none"> <li>◦ IEC 60950-1 and EN 60950-1.</li> </ul> </li> </ul>

**Table 83** Radio Specifications

FEATURE	DESCRIPTION
Media Access Protocol	IEEE 802.16e
WiMAX Bandwidth	3.4 GHz ~ 3.6 GHz (MAX218M2W) 2.496 GHz~2.690 GHz (MAX208M2W)
Data Rate	Aggregate throughput: up to 20 mbps Upload: 7 mbps
Modulation	QPSK (uplink and downlink) 16-QAM (uplink and downlink) 64-QAM (downlink only)
Output Power	Typically 26.5 dBm with internal antennas
Duplex mode	Time Division Duplex (TDD)
Security	PKMv2 EAP-TTLS/CHAP/PAP/MSCHAP/MSCHAPv2 CMAC message authentication CCM mode 128-bit AES data ciphering Device authentication WiMAX Forum X.509 certificates

**Table 84** Firmware Specifications

FEATURE	DESCRIPTION
Web-based Configuration and Management Tool	Also known as "the web configurator", this is a firmware-based management solution for the MAX208M2W Series. You must connect using a compatible web browser in order to use it.
High Speed Wireless Internet Access	The MAX208M2W Series is ideal for high-speed wireless Internet browsing.  WiMAX (Worldwide Interoperability for Microwave Access) is a wireless networking standard providing high-bandwidth, wide-range secured wireless service. The MAX208M2W Series is a WiMAX mobile station (MS) compatible with the IEEE 802.16e standard.
Firewall	The MAX208M2W Series is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The MAX208M2W Series's firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	The MAX208M2W Series can block access to web sites containing specified keywords. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering.

**Table 84** Firmware Specifications (continued)

FEATURE	DESCRIPTION
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
Universal Plug and Play (UPnP)	Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.
Dynamic DNS Support	With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.
DHCP	DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Your device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
Multiple SIP Accounts	You can configure multiple voice (SIP) accounts.
SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic (up to 60 ms). This helps ensure good voice quality for your conversations.
Voice Activity Detection/Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Echo Cancellation	Your device supports G.168 of at least 24 ms.  This an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Time and Date	Get the current time and date from an external server when you turn on your MAX208M2W Series. You can also set the time manually.

**Table 84** Firmware Specifications (continued)

FEATURE	DESCRIPTION
Logging	Use the MAX208M2W Series's logging feature to view connection history, surveillance logs, and error messages.
Codecs	G.711 (PCM $\mu$ -law and a-law), G729, G.729a
Fax Support	T.38 FAX relay (FAX over UDP). G.711 fax relay for fax calls and be able to renegotiate codec to G.711 if a fax call is detected.
Ring Tones	Supports different distinctive ring tones on each line.
Call Prioritization	Prioritize VoIP traffic originating from the RJ-11 ports over any other traffic.

**Table 85** Standards Supported

STANDARD	DESCRIPTION
RFC 768	User Datagram Protocol
RFC 791	Internet Protocol v4
RFC 792	Internet Control Message Protocol
RFC 792	Transmission Control Protocol
RFC 826	Address Resolution Protocol
RFC 854	Telnet Protocol
RFC 1112	IGMPv2
RFC 1349	Type of Service Protocol
RFC 1706	DNS NSAP Resource Records
RFC 1889	Real-time Transport Protocol (RTP)
RFC 1890	Real-time Transport Control Protocol (RTCP)
RFC 2030	Simple Network Time Protocol
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2236	IGMPv2
RFC 2131	Dynamic Host Configuration Protocol
RFC 2401	Security Architecture for the Internet Protocol
RFC 2409	Internet Key Exchange
RFC 2475	Architecture for Differentiated Services (Diffserv)
RFC 2543	SIP Protocol
RFC 2617	Hypertext Transfer Protocol (HTTP) Authentication: Basic and Digest Access Authentication
RFC 2782	A DNS RR for specifying the location of services (DNS SRV)
RFC 2833	Real-time Transport Protocol Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2976	The SIP INFO Method
RFC 3261	Session Initiation Protocol (SIP version 2)
RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP).

**Table 85** Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3323	A Privacy Mechanism for SIP
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3489	NAT Traversal - STUN
RFC 3550	RTP - A Real Time Protocol for Real-Time Applications
RFC 3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)-XR
RFC 3715	IP Sec/NAT Compatibility
RFC 3842	A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
IEEE 802.3	10BASE5 10 Mbit/s (1.25 MB/s)
IEEE 802.3u	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) with auto-negotiation

**Table 86** Voice Features

Call Park and Pickup	<p>Call park and pickup lets you put a call on hold (park) and then continue the call (pickup). The caller must still pay while the call is parked.</p> <p>When you park the call, you enter a number of your choice (up to eight digits), which you must enter again when you pick up the call. If you do not enter the correct number, you cannot pickup the call. This means that only someone who knows the number you have chosen can pick up the call.</p> <p>You can have more than one call on hold at the same time, but you must give each call a different number.</p>
Call Return	With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.
Country Code	Phone standards and settings differ from one country to another, so the settings on your MAX208M2W Series must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the MAX208M2W Series from one country to another.
Do not Disturb (DnD)	This feature allows you to set your phone not to ring when someone calls you. You can set each phone independently using its keypad, or configure global settings for all phones using the command line interpreter.

**Table 86** Voice Features

Auto Dial	You can set the MAX208M2W Series to automatically dial a specified number immediately whenever you lift a phone off the hook. Use the Web Configurator to set the specified number. Use the command line interpreter to have the MAX208M2W Series wait a specified length of time before dialing the number.
Phone config	The phone configuration table allows you to customize the phone keypad combinations you use to access certain features on the MAX208M2W Series, such as call waiting, call return, call forward, etc. The phone configuration table is configurable in command interpreter mode.
Firmware update enable / disable	If your service provider uses this feature, you hear a recorded message when you pick up the phone when new firmware is available for your MAX208M2W Series. Enter *99# in your phone's keypad to have the MAX208M2W Series upgrade the firmware, or enter #99# to not upgrade. If your service provider gave you different numbers to use, enter them instead. If you enter the code to not upgrade, you can make a call as normal. You will hear the recording again each time you pick up the phone, until you upgrade.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.
Call forwarding	With this feature, you can set the MAX208M2W Series to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
Caller ID	The MAX208M2W Series supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.

**Table 86** Voice Features

SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Other Voice Features	<p>SIP version 2 (Session Initiating Protocol RFC 3261)</p> <p>SDP (Session Description Protocol RFC 2327)</p> <p>RTP (RFC 1889)</p> <p>RTCP (RFC 1890)</p> <p>Voice codecs (coder/decoders) G.711, G.726, G.729</p> <p>Fax and data modem discrimination</p> <p>DTMF Detection and Generation</p> <p>DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO)</p> <p>Point-to-point call establishment between two IADs</p> <p>Quick dialing through predefined phone book, which maps the phone dialing number and destination URL.</p> <p>Flexible Dial Plan (RFC3525 section 7.1.14)</p>

**Table 87** Star (\*) and Pound (#) Code Support

*0	Wireless Operator Services
*2	Customer Care Access
*66	Repeat Dialing
*67	Plus the 10 digit phone number to block Caller ID on a single call basis
*69	Return last call received
*70	Followed by the 10 digit phone number to cancel Call Waiting on a single call basis
*72	Activate Call Forwarding (*72 followed by the 10 digit phone number that is requesting call forwarding service)
*720	Activate Call Forwarding (*720 followed by the 10 digit phone number that is requesting deactivation of call forwarding service)
*73	Plus the forward to phone number to activate Call Forwarding No Answer (no VM service plan)
*730	Deactivate Call Forwarding No Answer
*740	Plus the forward to phone number to activate Call Forwarding Busy (no VM service plan)
*911/911	Emergency phone number (same as dialing 911)
*411/411	Wireless Information Services

Note: To take full advantage of the supplementary phone services available through the MAX208M2W Series's phone port, you may need to subscribe to the services from your voice account service provider.

Not all features are supported by all service providers. Consult your service provider for more information.