

OX253P

WiMAX MIMO Outdoor Simple CPE

User's Guide

Default Login Details

IP Address: <http://192.168.1.1>

Administrator's
User Name and
Password: admin/admin

General User's
User Name and
Password: user/user

Firmware Version 3.70
Edition 1, 11/2010



ZTE中兴

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the OX253P using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

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

- Web Configurator Online Help

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

- Command Reference Guide

The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the OX253P.

Note: It is recommended you use the web configurator to configure the OX253P.

- Support Disc

Disclaimer

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

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 OX253P.

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 "OX253P", 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 OX253P icon is not an exact representation of your OX253P.

Table 1 Common Icons

WiMAX Access Point 	Computer 	Wireless Signal 
Notebook 	Server 	WiMAX Base Station 
Telephone 	Switch 	Router 
Internet Cloud 	Internet/WiMAX 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.



Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Contents Overview

User's Guide	17
Getting Started	19
Introducing the Web Configurator	23
Internet Connection Wizard	29
Tutorials	35
Technical Reference	45
The Setup Screens	47
The LAN Configuration Screens	53
The WAN Configuration Screens	65
The NAT Configuration Screens	77
The System Configuration Screens	87
The Certificates Screens	97
The Firewall Screens	119
Content Filter	129
The Remote Management Screens	133
QoS	145
The Logs Screens	149
The Status Screen	163
Troubleshooting	173
Product Specifications	181

Table of Contents

About This User's Guide	3
Document Conventions	4
Safety Warnings	6
Contents Overview	9
Table of Contents	11
Part I: User's Guide	17
Chapter 1	
Getting Started	19
1.1 About Your OX253P	19
1.1.1 WiMAX Internet Access	19
1.2 OX253P Hardware	20
1.2.1 LEDs	20
1.3 Good Habits for Managing the Device	21
Chapter 2	
Introducing the Web Configurator	23
2.1 Overview	23
2.1.1 Accessing the Web Configurator	23
2.2 The Main Screen	25
Chapter 3	
Internet Connection Wizard	29
3.1 Overview	29
3.1.1 Welcome to the Setup Wizard	29
3.1.2 System Information	30
3.1.3 Authentication Settings	31
3.1.4 IP Address	33
3.1.5 Setup Complete	34
Chapter 4	
Tutorials	35
4.1 Overview	35

4.2 Setting Up a Small Network	35
4.2.1 Connecting Your Small Network to the Internet	37
4.2.2 Changing Service Providers	37
4.2.3 Blocking Web Access During Specific Hours	39
4.2.4 Blocking Web Sites by Keyword	42
4.3 Remotely Managing Your OX253P	44
Part II: Technical Reference	45
Chapter 5	
The Setup Screens.....	47
5.1 Overview	47
5.1.1 What You Can Do in This Chapter	47
5.1.2 What You Need to Know	47
5.1.3 Before You Begin	48
5.2 Set IP Address	48
5.3 DHCP Client	49
5.4 Time Setting	50
5.4.1 Pre-Defined NTP Time Servers List	51
5.4.2 Resetting the Time	52
Chapter 6	
The LAN Configuration Screens.....	53
6.1 Overview	53
6.1.1 What You Can Do in This Chapter	53
6.1.2 What You Need to Know	53
6.2 DHCP Setup	54
6.3 Static DHCP	56
6.4 IP Static Route	57
6.4.1 IP Static Route Setup	58
6.5 Other Settings	59
6.6 Technical Reference	60
6.6.1 IP Address and Subnet Mask	61
6.6.2 DHCP Setup	61
6.6.3 LAN TCP/IP	62
6.6.4 DNS Server Address	62
6.6.5 RIP Setup	63
6.6.6 Multicast	63
Chapter 7	
The WAN Configuration Screens.....	65

7.1 Overview	65
7.1.1 What You Can Do in This Chapter	65
7.1.2 What You Need to Know	65
7.2 Internet Connection	68
7.3 WiMAX Configuration	70
7.3.1 Frequency Ranges	72
7.3.2 Configuring Frequency Settings	73
7.3.3 Using the WiMAX Frequency Screen	73
7.4 Buzzer	74
7.5 Advanced	75
Chapter 8	
The NAT Configuration Screens	77
8.1 Overview	77
8.1.1 What You Can Do in This Chapter	77
8.2 General	77
8.3 Port Forwarding	78
8.3.1 Port Forwarding Options	79
8.3.2 Port Forwarding Rule Setup	81
8.4 Trigger Port	82
8.4.1 Trigger Port Forwarding Example	84
8.5 ALG	85
Chapter 9	
The System Configuration Screens	87
9.1 Overview	87
9.1.1 What You Can Do in This Chapter	87
9.1.2 What You Need to Know	87
9.2 General	89
9.3 Dynamic DNS	90
9.4 Firmware	92
9.4.1 The Firmware Upload Process	93
9.5 Configuration	93
9.5.1 The Restore Configuration Process	94
9.6 Restart	95
9.6.1 The Restart Process	95
9.7 Bridge	95
Chapter 10	
The Certificates Screens	97
10.1 Overview	97
10.1.1 What You Can Do in This Chapter	97
10.1.2 What You Need to Know	97

10.2 My Certificates	98
10.2.1 My Certificates Create	100
10.2.2 My Certificate Edit	104
10.2.3 My Certificate Import	107
10.3 Trusted CAs	108
10.3.1 Trusted CA Edit	110
10.3.2 Trusted CA Import	113
10.4 Technical Reference	113
10.4.1 Certificate Authorities	114
10.4.2 Verifying a Certificate	116
Chapter 11	
The Firewall Screens	119
11.1 Overview	119
11.1.1 What You Can Do in This Chapter	119
11.1.2 What You Need to Know	119
11.2 Firewall Setting	120
11.2.1 Firewall Rule Directions	120
11.2.2 Triangle Route	121
11.2.3 Firewall Setting Options	122
11.3 Services	123
11.4 Technical Reference	124
11.4.1 Stateful Inspection Firewall	124
11.4.2 Guidelines For Enhancing Security With Your Firewall	125
11.4.3 The “Triangle Route” Problem	125
Chapter 12	
Content Filter.....	129
12.1 Overview	129
12.1.1 What You Can Do in This Chapter	129
12.2 Filter	130
12.3 Schedule	132
Chapter 13	
The Remote Management Screens	133
13.1 Overview	133
13.1.1 What You Can Do in This Chapter	133
13.1.2 What You Need to Know	134
13.2 WWW	135
13.3 Telnet	136
13.4 FTP	136
13.5 SNMP	137
13.5.1 SNMP Traps	138

13.5.2 SNMP Options	139
13.6 DNS	140
13.7 Security	141
13.8 CWMP-TR069	142
Chapter 14	
QoS.....	145
14.1 Overview	145
14.2 General	145
14.3 Class Setup	146
14.3.1 Class Configuration	147
Chapter 15	
The Logs Screens	149
15.1 Overview	149
15.1.1 What You Can Do in This Chapter	149
15.1.2 What You Need to Know	149
15.2 View Logs	151
15.3 Log Settings	153
15.4 Log Message Descriptions	155
Chapter 16	
The Status Screen.....	163
16.1 Overview	163
16.2 Status Screen	163
16.2.1 Packet Statistics	167
16.2.2 WiMAX Site Information	168
16.2.3 DHCP Table	169
16.2.4 WiMAX Profile	170
16.3 Technical Reference	171
Chapter 17	
Troubleshooting.....	173
17.1 Power, Hardware Connections, and LEDs	173
17.2 OX253P Access and Login	174
17.3 Internet Access	176
17.4 Export a Certificate File	178
17.5 Reset the OX253P to Its Factory Defaults	179
17.5.1 Pop-up Windows, JavaScripts and Java Permissions	179
Chapter 18	
Product Specifications	181
Appendix A WiMAX Security	185

Table of Contents

Appendix B Setting Up Your Computer's IP Address	189
Appendix C Pop-up Windows, JavaScripts and Java Permissions	217
Appendix D IP Addresses and Subnetting	229
Appendix E Importing Certificates	241
Appendix F Common Services	271
Index.....	275

PART I

User's Guide

Getting Started

1.1 About Your OX253P

The OX253P has a built-in switch and allows you to access the Internet by connecting to a WiMAX wireless network.

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

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

See [Chapter 18 on page 181](#) for a complete list of features for your model.

1.1.1 WiMAX Internet Access

Connect your computer or network to the OX253P for WiMAX Internet access. See the Quick Start Guide for instructions on hardware connection.

In a wireless metropolitan area network (MAN), the OX253P connects to a WiMAX base station (BS) for Internet access.

The following diagram shows a notebook computer equipped with the OX253P 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.

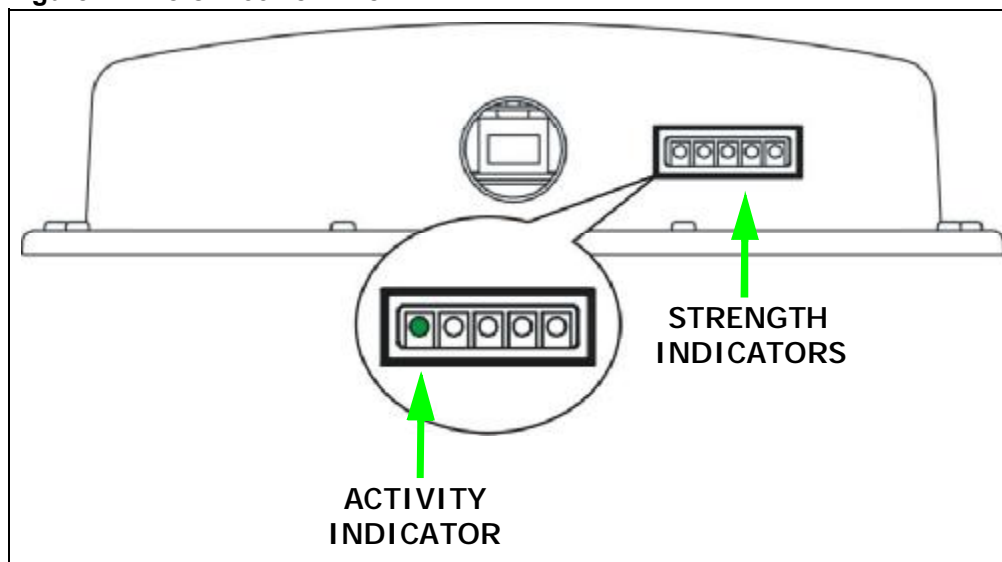
1.2 OX253P Hardware

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 OX253P.

Figure 2 The OX253P's LEDs



The following table describes your OX253P's LEDs (from right to left).

Table 2 The OX253P

LED	STATE	DESCRIPTION
Power (IDU only)	Off	The OX253P is not receiving power.
	Green	The OX253P is receiving power and functioning correctly.

Table 2 The OX253P

LED	STATE	DESCRIPTION
Strength Indicator	The Strength Indicator LEDs display the Received Signal Strength Indication (RSSI) of the wireless (WiMAX) connection.	
	5 Signal LEDs	The signal strength is greater than or equal to -59 dBm.
	4 Signal LEDs	The signal strength is between -69 and -60 dBm.
	3 Signal LEDs	The signal strength is between -79 and -70 dBm.
	2 Signal LEDs	The signal strength is between -89 and -90 dBm.
	1 Signal LED	The signal strength is between -90 and -95 dBm.
	0 Signal LEDs	There is no WiMAX connection.
Activity Indicator	Off	The OX253P is not ready.
	Green	The OX253P is connected to the network.
	Blinking	The OX253P system is booting up or the OX253P is seeking a viable signal.

1.3 Good Habits for Managing the Device

Do the following things regularly to make the OX253P more secure and to manage the OX253P 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 OX253P becomes unstable or even crashes. If you forget your password, you will have to reset the OX253P to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the OX253P. 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 217](#) for more information on configuring your web browser.

2.1.1 Accessing the Web Configurator

- 1 Make sure your OX253P 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 Select your preferable language from the language drop-down list.

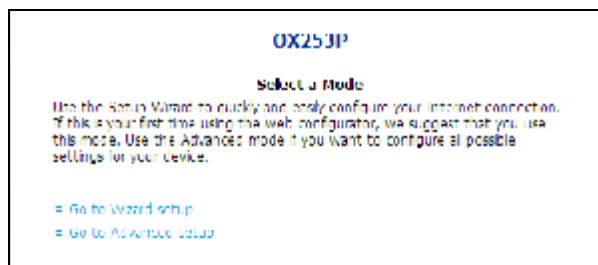
- 5 A password screen displays. Enter the default username (admin) and password (admin) and then click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.



- 6 The following screen displays. Click **Apply** to have the OX253P generate a new certificate. You can also click **Ignore** to have the OX253P use the default certificate.



- 7 A screen displays to let you choose to go to the Wizard or the Advanced screens.
 - Click **Go to Wizard setup** if you are logging in for the first time or if you want to make basic changes. The wizard selection screen appears. See [Chapter 3 on page 29](#) for more information.
 - Click **Go to Advanced setup** if you want to configure features that are not available in the wizards. The main screen appears. See [Section 16.2 on page 163](#) for more information.
 - Click **Exit** if you want to log out.



Note: For security reasons, the OX253P automatically logs you out if you do not use the Web Configurator for five minutes. If this happens, log in again.

2.2 The Main Screen

When you first log into the web configurator and by-pass the wizard, the Main screen appears. Here you can view a summary of your OX253P 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.

Figure 3 Main Screen



The following table describes the icons in this screen.

Table 3 Main > Icons







ICON	DESCRIPTION
	<p>MAIN</p> <p>Click to return to the Main screen.</p>
	<p>SETUP</p> <p>Click to go the Setup screen, where you can configure LAN, DHCP and WAN settings.</p>

Table 3 Main > Icons (continued)

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

The following table describes the labels in this screen.

Table 4 Main

LABEL	DESCRIPTION
Wizard	Click to run the Internet Connection Setup Wizard. All of the settings that you can configure in this wizard are also available in these web configurator screens.
Logout	Click to log out of the web configurator. Note: This does not log you off the WiMAX network, it simply logs you out of the OX253P's browser-based configuration interface.
WiMAX Connection Status	<p>This field indicates the current status of your WiMAX connection.</p> <p>Status messages are as follows:</p> <ul style="list-style-type: none"> • Connected - Indicates that the OX253P is connected to the WiMAX network. Use the Strength Indicator icon to determine the quality of your network connection. • Disconnected - Indicates that the OX253P is not connected to the WiMAX network. • DL_SYN - Indicates a download synchronization is in progress. This means the firmware is checking with the server for any updates or settings alterations.

Table 4 Main (continued)

LABEL	DESCRIPTION
Software Version	<p>This field indicates the version number of the OX253P's firmware. The version number takes the form of: <i>Version(Build),release status (candidate) Version Release Date</i>.</p> <p>For example: V3.70(TPG.0)c4 07/08/2010 indicates that the firmware is 3.70, build TPG.0, candidate 4, released on July 08, 2010.</p>
Version Date	This field indicates the exact date and time the current firmware was compiled.
System Uptime	This field indicates how long the OX253P has been on. This resets every time you shut the device down or restart it.
WiMAX Uptime	This field indicates how long the OX253P has been connected to the WiMAX network. This resets every time you disconnect from the WiMAX network, shut the device down, or restart it.

Internet Connection Wizard

3.1 Overview

This chapter provides information on the Setup Wizard screens. The wizard guides you through several steps where you can configure your Internet settings.

3.1.1 Welcome to the Setup Wizard

This is the welcome screen for the Setup Wizard.

The Internet Connection Wizard screens are described in detail in the following sections.

Figure 4 Select a Mode



3.1.2 System Information

This Internet Connection Wizard screen allows you to configure your OX253P's system information. The settings here correspond to the **ADVANCED > System Configuration > General** screen (see [Section 9.2 on page 89](#) for more).

Figure 5 Internet Connection Wizard > System Information

System Information

Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.

System Name:

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below. This field is normally left blank.

Domain Name:

< Back Next > Close

The following table describes the labels in this screen.

Table 5 Internet Connection Wizard > System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the OX253P in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.
Close	Click to close the wizard without saving.

3.1.3 Authentication Settings

This Internet Connection Wizard screen allows you to configure your Internet access settings. The settings here correspond to the **ADVANCED > WAN Configuration > Internet Connection** screen (see [Section 7.2 on page 68](#) for more information).

Figure 6 Internet Connection Wizard > Authentication Settings Screen

The following table describes the labels in this screen.

Table 6 Internet Connection Wizard > Authentication Settings Screen

LABEL	DESCRIPTION
User Name	Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters.
Password	Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters.
Anonymous Identity	Enter the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption. The anonymous identity is used to route your authentication request to the correct authentication server, and does not reveal your real user name. Your real user name and password are encrypted in the TLS tunnel, and only the anonymous identity can be seen. Leave this field blank if your ISP did not give you an anonymous identity to use.
PKM	This field displays the Privacy Key Management version number. PKM provides security between the OX253P and the base station. At the time of writing, the OX253P supports PKMv2 only. See the WiMAX security appendix for more information.

Table 6 Internet Connection Wizard > Authentication Settings Screen (continued)

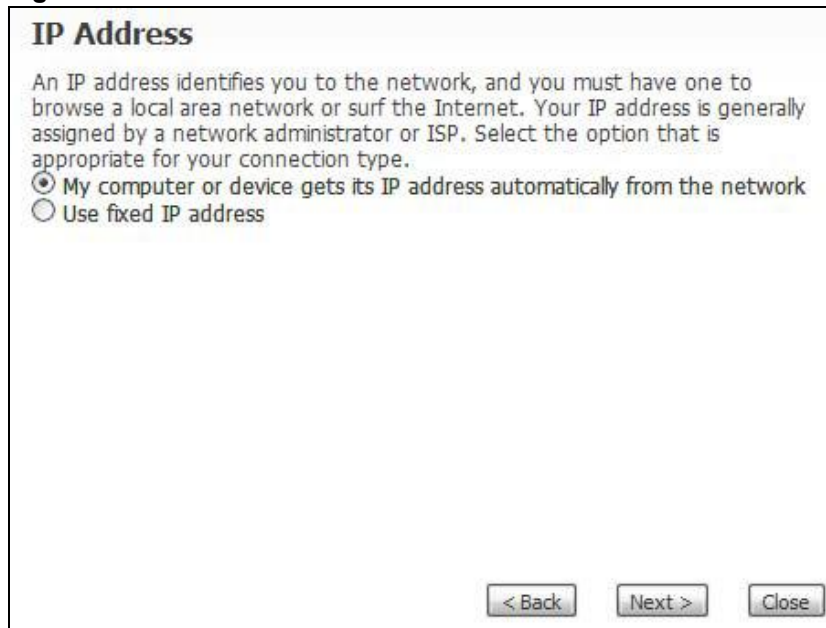
LABEL	DESCRIPTION
Authentication	<p>This field displays the user authentication method. Authentication is the process of confirming the identity of a mobile station (by means of a username and password, for example).</p> <p>Check with your service provider if you are unsure of the correct setting for your account.</p> <p>Choose from the following user authentication methods:</p> <ul style="list-style-type: none"> • TTLS (Tunnelled Transport Layer Security) • TLS (Transport Layer Security) <p>Note: Not all OX253Ps support TLS authentication. Check with your service provider for details.</p>
TTLS Inner EAP	<p>This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details. The OX253P supports the following inner authentication types:</p> <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol)
Certificate	<p>This is the security certificate the OX253P uses to authenticate the AAA server. Use the TOOLS > Certificates > Trusted CA screen to import certificates to the OX253P.</p>
Back	<p>Click to display the previous screen.</p>
Next	<p>Click to proceed to the next screen.</p>
Close	<p>Click to close the wizard without saving.</p>

3.1.4 IP Address

This Internet Connection Wizard screen allows you to configure your IP address. The settings here correspond to the **SETUP > Set IP Address** screen (see [Section 5.2 on page 48](#)).

A fixed IP address is a static IP that your ISP gives you. An automatic (dynamic) IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.

Figure 7 Internet Connection Wizard > IP Address



The following table describes the labels in this screen.

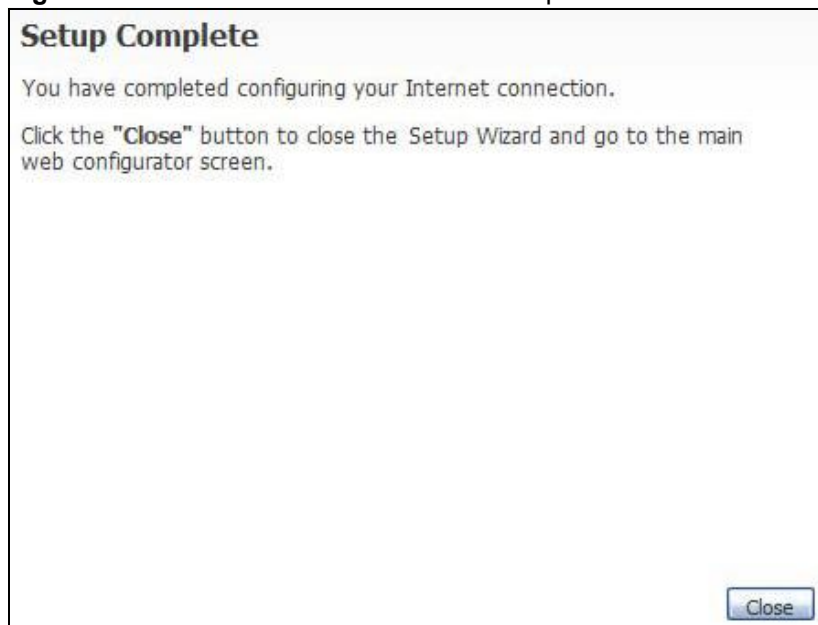
Table 7 Internet Connection Wizard > IP Address

LABEL	DESCRIPTION
IP Address	
My computer or device gets its IP address automatically from the network	Select this if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Use fixed IP Address	A static IP address is a fixed IP that your ISP gives you.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.
Close	Click to close the wizard screen without saving.

3.1.5 Setup Complete

Click **Close** to complete and save the Internet Connection Wizard settings.

Figure 8 Internet Connection Wizard > Complete



Launch your web browser and navigate to a website of your choice . 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 OX253P 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

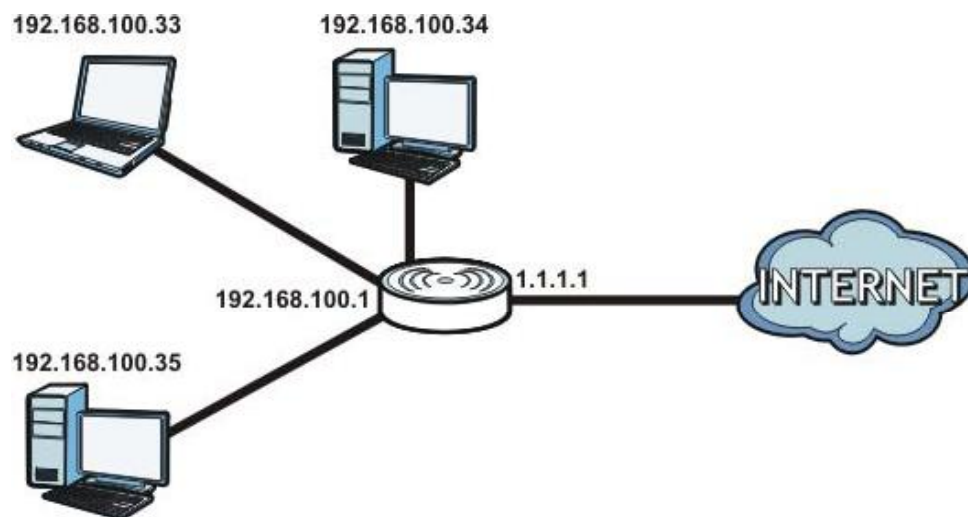
This chapter shows you how to configure some of the OX253P's features.

Note: Be sure to read [Introducing the Web Configurator on page 23](#) before working through the tutorials presented here. For field descriptions of individual screens, see the related technical reference in this User's Guide.

4.2 Setting Up a Small Network

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

Goal: Connect three computers to your OX253P 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	Chapter 5 on page 47
Starting IP Address	192.168.100.33	Chapter 6 on page 53
Pool Size	32	
DNS Servers	From ISP	

- 1 In the Web Configurator, open the **SETUP > Set IP Address** screen and set the IP Address to 192.168.100.1. Use the default IP Subnet Mask of 255.255.255.0.

Set IP Address

IP Address:

IP Subnet Mask:

- 2 Open the **ADVANCED > LAN Configuration > DHCP Setup** screen.

DHCP Setup

Enable DHCP Server

IP Pool Starting Address: Pool Size:

DNS Server

DNS Servers Assigned by DHCP Server:

First DNS Server:

Second DNS Server:

Third DNS Server:

- 3 Select **Enable DHCP Server**, then enter 192.168.100.34 as your **IP Pool Starting Address** and 32 for your **Pool Size**.
- 4 In the **DNS Server** section, set the **First**, **Second** and **Third DNS Server** fields to **From ISP** in order to use the DNS servers linked to your ISP.
- 5 Click **Apply** to save your DHCP settings.

- Next, go to the **ADVANCED > NAT Configuration > General** screen and select the **Enable Network Address Translation** option.



The screenshot shows a web interface for NAT Configuration. The 'General' tab is active. Under the 'General' section, the checkbox for 'Enable Network Address Translation' is checked. Below it, the 'Max NAT/Firewall Session Per User' is set to 512. At the bottom right, there are 'Apply' and 'Reset' buttons.

- Click **Apply** to save your settings.
- Connect your computers to the OX253P'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 189](#).

4.2.1 Connecting Your Small Network to the Internet

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 29](#)), which walks you through the process.

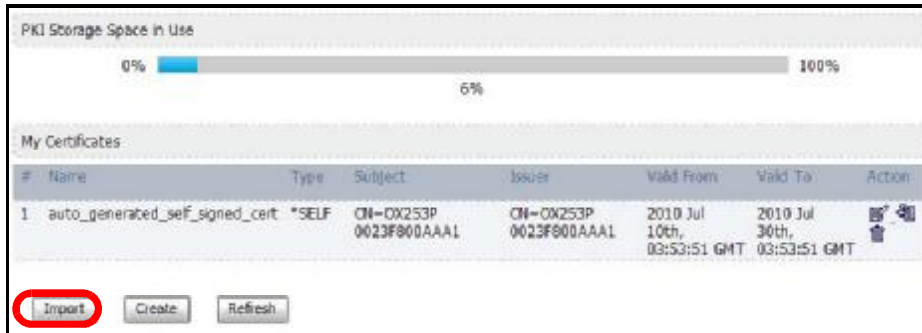
4.2.2 Changing Service Providers

This tutorial shows you how to import a new security certificate, which allows your device to communicate with the company's network servers. This is necessary if you ever change Internet Service Providers and your OX253P is still compatible with the new network. (In some cases it may not be.)

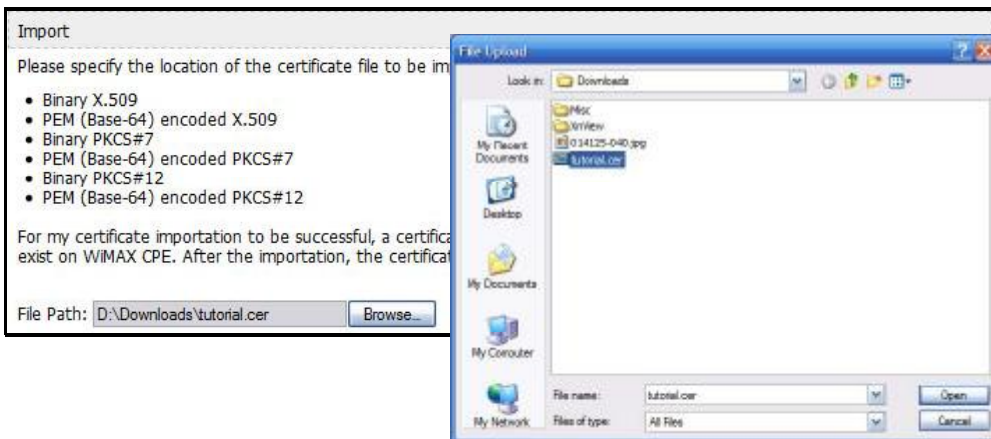
Goal: Import a new security certificate into the OX253P.

See Also: [Chapter 10 on page 97](#).

- 1 In the Web Configurator, open the **TOOLS > Certificates > My Certificates** screen and click the **Import** button.



- 2 In the **Import Certificate** screen, click **Browse** and locate the security certificate that was provided by your new ISP.



- 3 Next, go to the **ADVANCED > WAN Configuration** screen and configure your new Internet access settings based on the information provided by your ISP.

The screenshot shows the WAN Configuration screen with two main sections:

- ISP Parameters for Internet Access:**
 - User Name: abcd@example.com
 - Password: [masked]
 - Anonymous Identity: [empty]
 - PKM: PKMV2
 - Authentication: TTLS
 - TTLS Inner EAP: PAP
 - Certificate: tutorial** (highlighted with a red circle)
- WAN IP Address Assignment:**
 - Get automatically from ISP (Default)
 - Use Fixed IP Address
 - IP Address: 0.0.0.0
 - IP Subnet Mask: 0.0.0.0
 - Gateway IP Address: 0.0.0.0

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

- 4 From the **Certificates** menu, select the security certificate that you just imported.
- 5 Click **Apply** to save your settings. You should now be able to connect to the Internet through your new service provider!

4.2.3 Blocking Web Access During Specific Hours

If your OX253P is in a home or office environment you may decide that you want to block web access and video chat during a specific block of hours, such as during your daughter's designated study hours.

Goal: Configure the OX253P's firewall to block web and video chat access on weekdays between the hours of 3:30 PM and 8:30 PM.

See Also: [Chapter 11 on page 119](#).

1 Open the **TOOLS > Firewall > Services** to screen.

Service Setup

Enable Services Blocking

Available Services:

- Custom Port...
- Any(TCP)
- Any(UDP)
- IPSEC_TUNNEL(ESP:0)
- MULTICAST(IGMP:0)
- PING(ICMP:0)
- PPTP_TUNNEL(GRE:0)
- BGP(TCP:179)

Blocked Services:

Select "Custom Port", you can give new port range for blocking

Type: ~ ~

Schedule to Block

Day to Block

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Block (24-Hour Format)

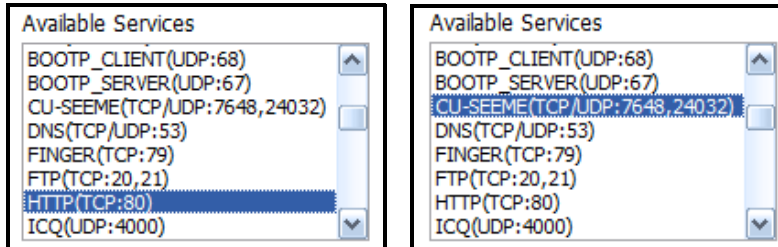
All day

From: Start (hour) (min) End (hour) (min)

2 Select **Enable Services Blocking**.

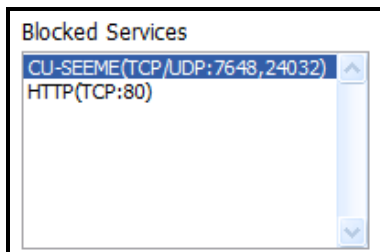
Enable Services Blocking

- 3 Under **Available Services**, select **HTTP(TCP:80)** then click the **Add** button. Repeat this for **CU-SEEME(TCP/UDP:7648,24032)**.

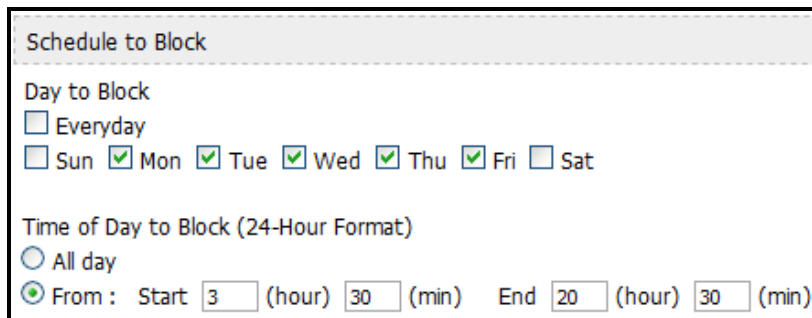


This blocks all web and video chat traffic, while leaving other ports open for other types of traffic, such as ports 25 and 587 for e-mail and port 21 for FTP.

The **Blocked Services** window updates accordingly.



- 4 Next, configure the **Schedule to Block** area with the days and hours for blocking web access to your employees.



In this example, the five weekly work days are selected as well as the standard work hours of 3:30 PM to 8:30 PM (or 20:30 in 24-hour format).

- 5 Finally, click **Apply** to save your settings.

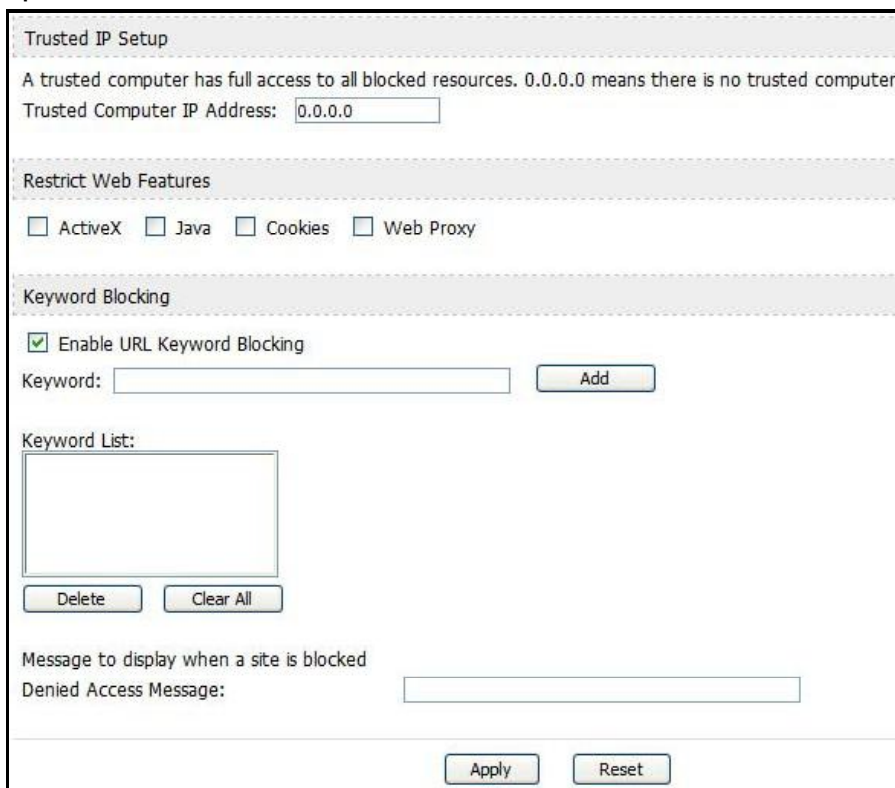
4.2.4 Blocking Web Sites by Keyword

You can further refine web access by specifying keywords that appear in a URL and blocking them. This allows you to control the content you do allow to pass through the OX253P. For example, once your daughter's designated study hours end, you allow web access and video chat but want to restrict certain sites.

Goal: Restrict websites with the words "poker", "sex", and "beer" in their URLs.

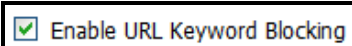
See Also: [Chapter 12 on page 129](#).

- 1 Open the **TOOLS > Content Filter > Filter** screen.



The screenshot shows the 'Trusted IP Setup' section with a text box for 'Trusted Computer IP Address' containing '0.0.0.0'. Below it is the 'Restrict Web Features' section with checkboxes for 'ActiveX', 'Java', 'Cookies', and 'Web Proxy', all of which are unchecked. The 'Keyword Blocking' section has the 'Enable URL Keyword Blocking' checkbox checked. Below this is a 'Keyword:' text box and an 'Add' button. A 'Keyword List:' text area is empty, with 'Delete' and 'Clear All' buttons below it. At the bottom, there is a 'Denied Access Message:' text box and 'Apply' and 'Reset' buttons.

- 2 Select **Enable URL Keyword Blocking**.



A close-up of the 'Enable URL Keyword Blocking' checkbox, which is checked.

- 3 Enter the first **Keyword** then click **Add**. Repeat for additional keywords.

Enable URL Keyword Blocking
 Keyword:

As you enter them, the keywords appear in the **Keyword List**.

Keyword List:
 poker
 sex
 beer

- 4 (Optional) If you want to allow websites with these keywords for a specific computer in your household, such as the computer in the master bedroom, then add that computer's IP address to the **Trusted IP Address** field.

Trusted IP Setup
 A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.
 Trusted Computer IP Address:

- 5 Click **Apply** to save these settings.
- 6 Next, open the **TOOLS > Content Filter > Schedule** screen.

Filter Schedule
 Day to Block:
 Everyday
 Sun Mon Tue Wed Thu Fri Sat
 Time of Day to Block: (24-Hour Format)
 All day
 From : Start (hour) (min) End (hour) (min)

- 7 To keep things simple, set the **Days to Block** to **Everyday** and the **Time of Day to Block** to **All Day**.
- 8 Click **Apply** to save these settings.


4.3 Remotely Managing Your OX253P

The remote management feature allows you to log into the device over the Internet and configure its settings from a second trusted location.

Goal: Set up the OX253P to allow management requests from the (demonstration) IP address 2.2.2.2.

See Also: [Chapter 13 on page 133](#).

- 1 Open the **TOOLS > Remote Management > WWW** screen.



The screenshot shows the 'Remote Management' configuration page. At the top, there are several tabs: 'WWW', 'Telnet', 'FTP', 'SNMP', 'DNS', 'Security', and 'CWMP-TR069'. The 'WWW' tab is selected. Below the tabs, there are three configuration fields: 'Server Port' with a text box containing '80', 'Server Access' with a dropdown menu showing 'WAN', and 'Secured Client IP Address' with radio buttons for 'All' and 'Selected' (which is selected), and a text box containing '2.2.2.2'. At the bottom right, there are two buttons: 'Apply' and 'Reset'.

- 2 Leave the **Server Port** setting as '80', in order to allow computers back at the OX253P's location to continue to access the Internet.
- 3 From the **Server Access** menu, select **WAN**. This allows remote management connections only from the Internet.
- 4 Finally, in the **Secured Client IP Address** field enter 2.2.2.2 as the IP address from which you will be connecting to the OX253P. Any other attempts by computer on the Internet to connect will be rejected because their IP addresses won't match the one specified here.
- 5 Click **Apply** to save your changes.

PART II

Technical Reference

5

The Setup Screens

5.1 Overview

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

5.1.1 What You Can Do in This Chapter

- The **Set IP Address** screen ([Section 5.2 on page 48](#)) lets you configure the OX253P's IP address and subnet mask.
- The **DHCP Client** screen ([Section 5.3 on page 49](#)) to view connection information for clients configured by the OX253P's internal DHCP server.
- The **Time Setting** screen ([Section 5.4 on page 50](#)) lets you configure your OX253P's time and date keeping settings.

5.1.2 What You Need to Know

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

LAN

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

IP Address

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

Subnet Mask

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

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

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.

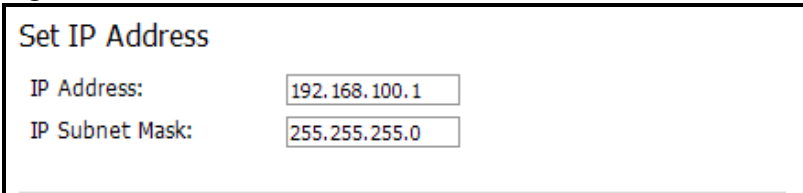
5.1.3 Before You Begin

- Make sure that you have made all the appropriate hardware connections to the OX253P, as described in the Quick Start Guide.
- Make sure that you have logged in to the web configurator at least one time and changed your password from the default, as described in the Quick Start Guide.

5.2 Set IP Address

Click the **SETUP** icon in the navigation bar to set up the OX253P's IP address and subnet mask. This screen displays this screen by default. If you are in any other sub-screen you can simply choose **Set IP Address** from the navigation menu on the left to open it again.

Figure 9 SETUP > Set IP Address



Set IP Address	
IP Address:	<input type="text" value="192.168.100.1"/>
IP Subnet Mask:	<input type="text" value="255.255.255.0"/>

The following table describes the labels in this screen.

Table 8 SETUP > Set IP Address

LABEL	DESCRIPTION
IP Address	Enter the IP address of the OX253P on the LAN. Note: This field is the IP address you use to access the OX253P on the LAN. If the web configurator is running on a computer on the LAN, you lose access to it as soon as you change this field and click Apply . You can access the web configurator again by typing the new IP address in the browser.
IP Subnet Mask	Enter the subnet mask of the LAN.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

5.3 DHCP Client

Click the **SETUP > DHCP Client** to view connection information for all clients that have been configured by the OX253P's internal DHCP server.

Figure 10 SETUP > Set IP Address

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	Coffee-Bean	00:1f:5b:ed:6c:7a	<input type="checkbox"/>
2	192.168.1.34	twpc13435	00:21:85:0c:44:1a	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 9 SETUP > Set IP Address

LABEL	DESCRIPTION
#	This indicates the number of the item in this list.
IP Address	This indicates the IP address of a connected client device.
Host Name	This indicates the host name of a connected client device. If the device is computer, then the host name is the computer name.
MAC Address	This indicates the MAC address of a connected client device.

Table 9 SETUP > Set IP Address (continued)

LABEL	DESCRIPTION
Reserve	This indicates whether the IP address for the connected client device is reserved. When the DHCP server issues IP addresses, reserved IPs are assigned to specific client devices. If the IP address is reserved, the client device identified by its MAC address will always receive this IP address from the DHCP server.
Apply	Click to save your changes.
Refresh	Click to refresh the information in the screen.

5.4 Time Setting

Click **SETUP > Time Setting** to set the date, time, and time zone for the OX253P.

Figure 11 SETUP > Time Setting

The following table describes the labels in this screen.

Table 10 SETUP > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	Displays the current time according to the OX253P.

Table 10 SETUP > Time Setting (continued)

LABEL	DESCRIPTION
Current Date	Displays the current time according to the OX253P.
Time and Date Setup	
Manual	Select this if you want to specify the current date and time in the fields below.
New Time	Enter the new time in this field, and click Apply .
New Date	Enter the new date in this field, and click Apply .
Get from Time Server	Select this if you want to use a time server to update the current date and time in the OX253P.
Time Protocol	Select the time service protocol that your time server uses. Check with your ISP or network administrator, or use trial-and-error to find a protocol that works. Daytime (RFC-867) - This format is day/month/year/time zone. Time (RFC-868) - This format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC-1305) - This format is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Select the time zone at your location.
Daylight Savings	Select this if your location uses daylight savings time. Daylight savings is a period from late spring to early fall when many places set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter which hour on which day of which week of which month daylight-savings time starts.
End Date	Enter which hour on the which day of which week of which month daylight-savings time ends.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

5.4.1 Pre-Defined NTP Time Servers List

The OX253P uses a pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified. It can use this list regardless of the time protocol you select.

When the OX253P uses the list, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then it goes through the rest of

the list in order until either it is successful or all the pre-defined NTP time servers have been tried.

Table 11 Pre-defined NTP Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

5.4.2 Resetting the Time

The OX253P automatically resets the time in the following circumstances:

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

The LAN Configuration Screens

6.1 Overview

Use the **ADVANCED > LAN Configuration** screens to set up the OX253P on the LAN. You can configure its IP address and subnet mask, DHCP services, and other subnets. You can also control how the OX253P sends routing information using RIP.

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

6.1.1 What You Can Do in This Chapter

- The **DHCP Setup** screen ([Section 6.2 on page 54](#)) lets you enable, disable, and configure the DHCP server in the OX253P.
- The **Static DHCP** screen ([Section 6.3 on page 56](#)) lets you assign specific IP addresses to specific computers on the LAN.
- The **IP Static Route** screen ([Section 6.4 on page 57](#)) lets you examine the static routes configured in the OX253P.
- The **Other Settings** screen ([Section 6.5 on page 59](#)) lets you control the routing information that is sent and received by each subnet assign specific IP addresses to specific computers on the LAN.

6.1.2 What You Need to Know

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

IP Address

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

Subnet Masks

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

DNS

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

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your OX253P an IP address, subnet mask, DNS and other routing information when it's turned on.

6.2 DHCP Setup

Click **ADVANCED > LAN Configuration > DHCP Setup** to enable, disable, and configure the DHCP server in the OX253P.

Figure 12 ADVANCED > LAN Configuration > DHCP Setup

The screenshot shows the DHCP Setup configuration interface. It includes a section for enabling the DHCP server and setting the IP pool, and another section for configuring DNS servers. The 'Enable DHCP Server' checkbox is checked. The IP Pool Starting Address is 192.168.100.33 and the Pool Size is 32. The DNS Servers Assigned by DHCP Server section shows three servers, each set to 'From ISP' and '0.0.0.0'. There are 'Apply' and 'Reset' buttons at the bottom.

The following table describes the labels in this screen.

Table 12 ADVANCED > LAN Configuration > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
Enable DHCP Server	Select this if you want the OX253P to be the DHCP server on the LAN. As a DHCP server, the OX253P assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information.

Table 12 ADVANCED > LAN Configuration > DHCP Setup (continued)

LABEL	DESCRIPTION
IP Pool Starting Address	Enter the IP address from which the OX253P begins allocating IP addresses, if you have not specified an IP address for this computer in ADVANCED > LAN Configuration > Static DHCP .
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by a subnet mask of 255.255.255.0 (regardless of the subnet the OX253P is in). For example, if the IP Pool Start Address is 10.10.10.10, the OX253P can allocate up to 10.10.10.254, or 245 IP addresses.
DNS Server	
First, Second and Third DNS Server	<p>Specify the IP addresses of a maximum of three DNS servers that the network can use. The OX253P provides these IP addresses to DHCP clients. You can specify these IP addresses two ways.</p> <p>From ISP - provide the DNS servers provided by the ISP on the WAN port.</p> <p>User Defined - enter a static IP address.</p> <p>DNS Relay - this setting will relay DNS information from the DNS server obtained by the OX253P.</p> <p>None - no DNS service will be provided by the OX253P.</p>
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

6.3 Static DHCP

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

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

Figure 13 ADVANCED > LAN Configuration > Static DHCP

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

The following table describes the labels in this screen.

Table 13 ADVANCED > LAN Configuration > Static DHCP

































LABEL	DESCRIPTION
#	The number of the item in this list.
MAC Address	Enter the MAC address of the computer to which you want the OX253P to assign the same IP address.
IP Address	Enter the IP address you want the OX253P to assign to the computer.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

6.4 IP Static Route

Click **ADVANCED > LAN Configuration > IP Static Route** to look at the static routes configured in the OX253P.



Note: The first static route is the default route and cannot be modified or deleted.

Figure 14 Advanced> LAN Configuration > IP Static Route

#	Name	Active	Destination	Gateway	Action
1	-	-	 
2	-	-	 
3	-	-	 
4	-	-	 
5	-	-	 
6	-	-	 
7	-	-	 
8	-	-	 
9	-	-	 
10	-	-	 
11	-	-	 
12	-	-	 
13	-	-	 
14	-	-	 
15	-	-	 
16	-	-	 

The following table describes the icons in this screen.

Table 14 Advanced> LAN Configuration > IP Static Route

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

The following table describes the labels in this screen.

Table 15 Advanced> LAN Configuration > IP Static Route

LABEL	DESCRIPTION
#	The number of the item in this list.
Name	This field displays the name that describes the static route.

Table 15 Advanced> LAN Configuration > IP Static Route (continued)

LABEL	DESCRIPTION
Active	This field shows whether this static route is active (Yes) or not (No).
Destination	This field displays the destination IP address(es) that this static route affects.
Gateway	This field displays the IP address of the gateway to which the OX253P should send packets for the specified Destination. The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Action	Click the Edit icon to modify this item. Click the Delete icon to remove this item.

6.4.1 IP Static Route Setup

Click an Edit icon in **ADVANCED > LAN Configuration > IP Static Route** to edit a static route in the OX253P.

Figure 15 Advanced> LAN Configuration > IP Static Route Setup > Edit

The following table describes the labels in this screen.

Table 16 Advanced> LAN Configuration > IP Static Route Setup > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the static route.
Active	Select this if you want the static route to be used. Clear this if you do not want the static route to be used.
Private	Select this if you do not want the OX253P to tell other routers about this static route. For example, you might select this if the static route is in your LAN. Clear this if you want the OX253P to tell other routers about this static route.
Destination IP Address	Enter one of the destination IP addresses that this static route affects.

Table 16 Advanced > LAN Configuration > IP Static Route Setup > Edit (continued)

LABEL	DESCRIPTION
IP Subnet Mask	Enter the subnet mask that defines the range of destination IP addresses that this static route affects. If this static route affects only one IP address, enter 255.255.255.255.
Gateway IP Address	Enter the IP address of the gateway to which the OX253P should send packets for the specified Destination. The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Usually, you should keep the default value. This field is related to RIP. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the metric, the lower the "cost". RIP uses hop count as the measurement of cost, where 1 is for a directly-connected network. The metric must be 1-15; if you use a value higher than 15, the routers assume the link is down.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

6.5 Other Settings

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

Figure 16 ADVANCED > LAN Configuration > Other Settings

RIP & Multicast Setup

RIP Direction: Both

RIP Version: RIP-1

Multicast: None

Apply Reset

The following table describes the labels in this screen.

Table 17 ADVANCED > LAN Configuration > Other Settings

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	<p>Use this field to control how much routing information the OX253P sends and receives on the subnet.</p> <ul style="list-style-type: none"> • None - The OX253P does not send or receive routing information on the subnet. • Both - The OX253P sends and receives routing information on the subnet. • In Only - The OX253P only receives routing information on the subnet. • Out Only - The OX253P only sends routing information on the subnet.
RIP Version	<p>Select which version of RIP the OX253P uses when it sends or receives information on the subnet.</p> <ul style="list-style-type: none"> • RIP-1 - The OX253P uses RIPv1 to exchange routing information. • RIP-2B - The OX253P broadcasts RIPv2 to exchange routing information. • RIP-2M - The OX253P multicasts RIPv2 to exchange routing information.
Multicast	<p>You do not have to enable multicasting to use RIP-2M. (See RIP Version.)</p> <p>Select which version of IGMP the OX253P uses to support multicasting on the LAN. Multicasting sends packets to some computers on the LAN and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer).</p> <ul style="list-style-type: none"> • None - The OX253P does not support multicasting. • IGMP-v1 - The OX253P supports IGMP version 1. • IGMP-v2 - The OX253P supports IGMP version 2. <p>Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the LAN have to support the same version of IGMP.</p>
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

6.6 Technical Reference

The following section contains additional technical information about the OX253P features described in this chapter.

6.6.1 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the OX253P. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your OX253P, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your OX253P will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the OX253P unless you are instructed to do otherwise.

6.6.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the OX253P as a DHCP server or disable it. When configured as a server, the OX253P provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else each computer must be manually configured.

The OX253P is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see [Section 6.3 on page 56](#).

6.6.3 LAN TCP/IP

The OX253P has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

The LAN parameters of the OX253P are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see [Section 6.3 on page 56](#).

6.6.4 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

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

Some ISPs choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The OX253P supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in the **LAN Setup** screen are not specified, for instance, left as 0.0.0.0, the OX253P tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the OX253P, the OX253P forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen. This way, the OX253P can pass the DNS servers to the computers and the computers can query the DNS server directly without the OX253P's intervention.

6.6.5 RIP Setup

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

- **Both** - the OX253P will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the OX253P will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the OX253P will send out RIP packets but will not accept any RIP packets received.
- **None** - the OX253P 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 OX253P 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.

6.6.6 Multicast

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

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

The OX253P supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the OX253P queries all directly connected networks to gather group membership. After that, the OX253P periodically updates this

information. IP multicasting can be enabled/disabled on the OX253P LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

The WAN Configuration Screens

7.1 Overview

Use the **ADVANCED > WAN Configuration** screens to set up your OX253P's Wide Area Network (WAN) or Internet features.

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

7.1.1 What You Can Do in This Chapter

- The **Internet Connection** screen ([Section 7.2 on page 68](#)) lets you set up your OX253P's Internet settings.
- The **WiMAX Configuration** screen ([Section 7.3 on page 70](#)) lets set up the frequencies used by your OX253P.
- The **Advanced** screen ([Section 7.5 on page 75](#)) lets configure your DNS server, RIP, Multicast and Windows Networking settings.

7.1.2 What You Need to Know

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

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is the IEEE 802.16 wireless networking standard, which provides high-bandwidth, wide-range wireless service across wireless Metropolitan Area Networks (MANs).

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 17 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 18 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 OX253P and the base station are controlled by the base station. The OX253P 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 19 Using an AAA Server



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

7.2 Internet Connection

Click **ADVANCED > WAN Configuration** to set up your OX253P's Internet settings.

Note: Not all OX253P models have all the fields shown here.

Figure 20 ADVANCED > WAN Configuration > Internet Connection

The following table describes the labels in this screen.

Table 18 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
User Name	Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters.
Password	Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters.

Table 18 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access (continued)

LABEL	DESCRIPTION
Anonymous Identity	<p>Enter the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption. The anonymous identity is used to route your authentication request to the correct authentication server, and does not reveal your real user name. Your real user name and password are encrypted in the TLS tunnel, and only the anonymous identity can be seen.</p> <p>Leave this field blank if your ISP did not give you an anonymous identity to use.</p>
PKM	<p>This field displays the Privacy Key Management version number. PKM provides security between the OX253P and the base station. At the time of writing, the OX253P supports PKMv2 only. See the WiMAX security appendix for more information.</p>
Authentication	<p>This field displays the user authentication method. Authentication is the process of confirming the identity of a mobile station (by means of a username and password, for example).</p> <p>Check with your service provider if you are unsure of the correct setting for your account.</p> <p>Choose from the following user authentication methods:</p> <ul style="list-style-type: none"> • TTLS (Tunnelled Transport Layer Security) • TLS (Transport Layer Security) <p>Note: Not all OX253Ps support TLS authentication. Check with your service provider for details.</p>
TTLS Inner EAP	<p>This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details.</p> <p>This field is available only when TTLS is selected in the Authentication field.</p> <p>The OX253P supports the following inner authentication types:</p> <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol)
Auth Mode	<p>Select the authentication mode from the drop-down list box.</p> <p>This field is not available in all OX253Ps. Check with your service provider for details.</p> <p>The OX253P supports the following authentication modes:</p> <ul style="list-style-type: none"> • User Only • Device Only with Cert • Certs and User Authentication

Table 18 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access (continued)

LABEL	DESCRIPTION
Certificate	This is the security certificate the OX253P uses to authenticate the AAA server. Use the TOOLS > > Trusted CAs screen to import certificates to the OX253P.
WAN IP Address Assignment	
Get automatically from ISP (Default)	Select this if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Use Fixed IP Address	A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the IP Address field below.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

7.3 WiMAX Configuration

Click **ADVANCED > WAN Configuration > WiMAX Configuration** to set up the frequencies used by your OX253P.

In a WiMAX network, a mobile or subscriber station must use a radio frequency supported by the base station to communicate. When the OX253P looks for a connection to a base station, it can search a range of frequencies.

Radio frequency is measured in Hertz (Hz).

Table 19 Radio Frequency Conversion

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

Figure 21 ADVANCED > WAN Configuration >WiMAX Configuration

DL Frequency [1]:	<input type="text" value="2665500"/>	kHz
DL Frequency [2]:	<input type="text" value="2675500"/>	kHz
DL Frequency [3]:	<input type="text" value="2685500"/>	kHz
DL Frequency [4]:	<input type="text" value="0"/>	kHz
DL Frequency [5]:	<input type="text" value="0"/>	kHz
DL Frequency [6]:	<input type="text" value="0"/>	kHz
DL Frequency [7]:	<input type="text" value="0"/>	kHz
DL Frequency [8]:	<input type="text" value="0"/>	kHz
DL Frequency [9]:	<input type="text" value="0"/>	kHz
DL Frequency [10]:	<input type="text" value="0"/>	kHz
DL Frequency [11]:	<input type="text" value="0"/>	kHz
DL Frequency [12]:	<input type="text" value="0"/>	kHz
DL Frequency [13]:	<input type="text" value="0"/>	kHz
DL Frequency [14]:	<input type="text" value="0"/>	kHz
DL Frequency [15]:	<input type="text" value="0"/>	kHz
DL Frequency [16]:	<input type="text" value="0"/>	kHz
DL Frequency [17]:	<input type="text" value="0"/>	kHz
DL Frequency [18]:	<input type="text" value="0"/>	kHz
DL Frequency [19]:	<input type="text" value="0"/>	kHz
Bandwidth :	<input type="text" value="10000"/>	KHz

The following table describes the labels in this screen.

Table 20 ADVANCED > WAN Configuration >WiMAX Configuration

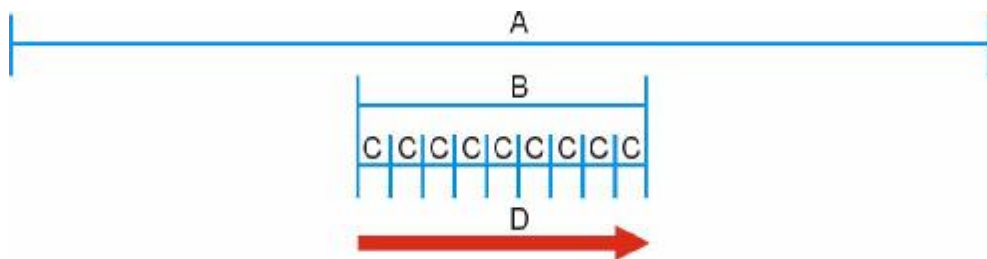
LABEL	DESCRIPTION
DL Frequency / Bandwidth	<p>These fields show the downlink frequency settings in kilohertz (kHz). Enter values in these fields to have the OX253P scan these frequencies for available channels in ascending numerical order.</p> <p>Note: The Bandwidth field is not user-configurable; when the OX253P finds a WiMAX connection, its frequency is displayed in this field.</p> <p>Contact your service provider for details of supported frequencies.</p>

Table 20 ADVANCED > WAN Configuration > WiMAX Configuration (continued)

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

7.3.1 Frequency Ranges

The following figure shows the OX253P 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 OX253P 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 OX253P searching for a connection.

Have the OX253P 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 OX253P searches for an available connection. Use the **Site Survey** screen to set these bands. You can set the downlink frequencies anywhere within the WiMAX frequency range. In this example, the downlink frequencies have been set to search all of the operator range for a connection.

7.3.2 Configuring Frequency Settings

You need to set the OX253P to scan one or more specific radio frequencies to find an available connection to a WiMAX base station.

Use the **WiMAX Frequency** screen to define the radio frequencies to be searched for available wireless connections. See [Section 7.3.3 on page 73](#) for an example of using the **WiMAX Frequency** screen.

Note: It may take several minutes for the OX253P to find a connection.

- The OX253P searches the **DL Frequency** settings in ascending numerical order, from [1] to [9].

Note: The **Bandwidth** field is not user-configurable; when the OX253P finds a WiMAX connection, its frequency is displayed in this field.

- If you enter a 0 in a **DL Frequency** field, the OX253P immediately moves on to the next **DL Frequency** field.
- When the OX253P connects to a base station, the values in this screen are automatically set to the base station's frequency. The next time the OX253P searches for a connection, it searches only this frequency. If you want the OX253P to search other frequencies, enter them in the **DL Frequency** fields.

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

Table 21 DL Frequency Example Settings

	EXAMPLE 1	EXAMPLE 2
DL Frequency [1]	2500000	2500000
DL Frequency [2]	2550000	2550000
DL Frequency [3]	0	2600000
DL Frequency [4]	0	0
DL Frequency [5]	0	0
	The OX253P searches at 2500000 kHz, and then searches at 2550000 kHz if it has not found a connection.	<i>The OX253P searches at 2500000 kHz and then at 2550000 kHz if it has not found an available connection. If it still does not find an available connection, it searches at 2600000 kHz.</i>

7.3.3 Using the WiMAX Frequency Screen

In this example, your Internet service provider has given you a list of supported frequencies: 2.51, 2.525, 2.6, and 2.625.

- 1 In the **DL Frequency [1]** field, enter 2510000 (2510000 kilohertz (kHz) is equal to 2.51 gigahertz).

- 2 In the DL Frequency [2] field, enter 2525000.
- 3 In the DL Frequency [3] field, enter 2600000.
- 4 In the DL Frequency [4] field, enter 2625000.

Leave the rest of the DL Frequency fields at zero. The screen appears as follows.

Figure 23 Completing the WiMAX Frequency Screen

DL Frequency [1]:	<input type="text" value="2510000"/>	kHz
DL Frequency [2]:	<input type="text" value="2525000"/>	kHz
DL Frequency [3]:	<input type="text" value="2600000"/>	kHz
DL Frequency [4]:	<input type="text" value="2625000"/>	kHz

- 5 Click **Apply**. The OX253P stores your settings.

When the OX253P searches for available frequencies, it scans all frequencies from DL Frequency [1] to DL Frequency [4]. When it finds an available connection, the fields in this screen will be automatically set to use that frequency.

7.4 Buzzer

Click **ADVANCED > WAN Configuration > Buzzer** to enable or disable buzzer in the ODU. The buzzer sounds beeps when the OX253P receives signal from the connected base station.

Figure 24 ADVANCED > WAN Configuration > Buzzer

Set the Buzzer Switch	
<input type="radio"/>	Enable Buzzer
<input checked="" type="radio"/>	Disable Buzzer
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The following table describes the labels in this screen.

Table 22 ADVANCED > WAN Configuration > Buzzer

LABEL	DESCRIPTION
Enable Buzzer	<p>Select this to turn on the buzzer in the outdoor unit (ODU). You may need to turn on the buzzer when you set up the ODU. The buzzer sounds the number of beeps based on the signal strength (the RSSI value) received from the base station.</p> <ul style="list-style-type: none"> • RSSI > -50: The five LEDs on the ODU light on and the buzzer sounds five beeps regularly. • -50 > RSSI > -60: Four of the five LEDs on the ODU light on and the buzzer sounds four beeps regularly. • -60 > RSSI > -70: Three of the five LEDs on the ODU light on and the buzzer sounds three beeps regularly. • -70 > RSSI > -80: Two of the five LEDs on the ODU light on and the buzzer sounds two beeps regularly. • -80 > RSSI > -90: One of the five LEDs on the ODU lights on and the buzzer sounds one beep regularly. • -90 > RSSI - The buzzer does not sound.
Disable Buzzer	Select this to turn the buzzer off.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

7.5 Advanced

Click **ADVANCED > WAN Configuration > Advanced** to configure your DNS server, RIP, Multicast and Windows Networking settings.

Figure 25 ADVANCED > WAN Configuration > Advanced

The screenshot shows the 'Advanced' configuration screen for WAN. It is divided into three sections: 'DNS Servers', 'Multicast Setup', and 'Windows Networking (NetBIOS over TCP/IP)'.
 - **DNS Servers:** Three rows for 'First DNS Server', 'Second DNS Server', and 'Third DNS Server'. Each row has a dropdown menu set to 'From ISP' and a text input field containing '0.0.0.0'.
 - **Multicast Setup:** A 'Multicast:' label followed by a dropdown menu set to 'None'.
 - **Windows Networking (NetBIOS over TCP/IP):** A checkbox labeled 'Allow between LAN and WAN (you also need to create a firewall rule!)' which is checked.
 At the bottom right, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 23 ADVANCED > WAN Configuration > Advanced

LABEL	DESCRIPTION
DNS Servers	
First, Second and Third DNS Server	<p>Select Obtained from ISP if your ISP dynamically assigns DNS server information (and the OX253P's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.</p> <p>Select UserDefined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose UserDefined, but leave the IP address set to 0.0.0.0, UserDefined changes to None after you click Apply. If you set a second choice to UserDefined, and enter the same IP address, the second UserDefined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. You must have another DHCP server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Multicast Setup	
Multicast	<p>IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The OX253P supports both IGMP version 1 (IGMP-v1) and IGMP-v2. Select None to disable it.</p>
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p>
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

The NAT Configuration Screens

8.1 Overview

Use these screens to configure port forwarding and trigger ports for the OX253P. You can also enable and disable SIP, FTP, and H.323 ALG.

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

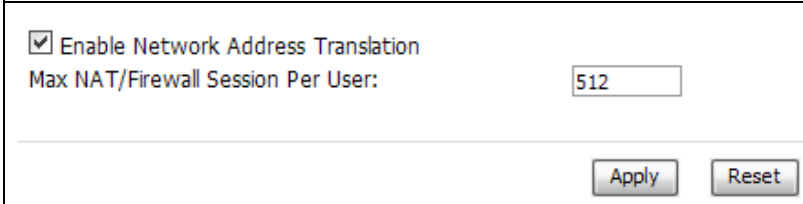
8.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 8.2 on page 77](#)) lets you enable or disable NAT and to allocate memory for NAT and firewall rules.
- The **Port Forwarding** screen ([Section 8.3 on page 78](#)) lets you look at the current port-forwarding rules in the OX253P, and to enable, disable, activate, and deactivate each one.
- The **Trigger Port** screen ([Section 8.4 on page 82](#)) lets you maintain trigger port forwarding rules for the OX253P.
- The **ALG** screen ([Section 8.5 on page 85](#)) lets you enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the OX253P.

8.2 General

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

Figure 26 ADVANCED > NAT Configuration > General



The screenshot shows a configuration window with a checked checkbox for "Enable Network Address Translation". Below it is a text input field for "Max NAT/Firewall Session Per User" containing the value "512". At the bottom right are "Apply" and "Reset" buttons.

The following table describes the labels in this screen.

Table 24 ADVANCED > NAT Configuration > General

LABEL	DESCRIPTION
Enable Network Address Translation	Select this if you want to use port forwarding, trigger ports, or any of the ALG.
Max NAT/Firewall Session Per User	<p>When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the OX253P.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.</p>
Apply	Click to save your changes.
Reset	Click to return to the previous screen without saving your changes.

8.3 Port Forwarding

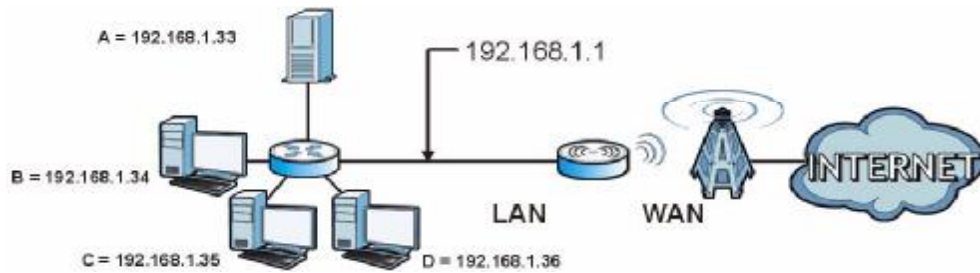
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

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

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

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

Figure 27 Multiple Servers Behind NAT Example



8.3.1 Port Forwarding Options



Click **ADVANCED > NAT Configuration > Port Forwarding** to look at the current port-forwarding rules in the OX253P, and to enable, disable, activate, and deactivate each one. You can also set up a default server to handle ports not covered by rules.

Figure 28 ADVANCED > NAT Configuration > Port Forwarding

Default Server Setup						
Default Server:		<input type="text" value="0.0.0.0"/>				
Port Forwarding						
#	Active	Name	Start Port	End Port	Server IP Address	Action
1	<input type="checkbox"/>		0	0		
2	<input type="checkbox"/>		0	0		
3	<input type="checkbox"/>		0	0		
4	<input type="checkbox"/>		0	0		
5	<input type="checkbox"/>		0	0		
6	<input type="checkbox"/>		0	0		
7	<input type="checkbox"/>		0	0		
8	<input type="checkbox"/>		0	0		
9	<input type="checkbox"/>		0	0		
10	<input type="checkbox"/>		0	0		
11	<input type="checkbox"/>		0	0		

The following table describes the icons in this screen.

Table 25 Advanced > VPN Transport > Customer Interface

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

The following table describes the labels in this screen.

Table 26 ADVANCED > NAT Configuration > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	Enter the IP address of the server to which the OX253P should forward packets for ports that are not specified in the Port Forwarding section below or in the TOOLS > Remote MGMT screens. Enter 0.0.0.0 if you want the OX253P to discard these packets instead.
Port Forwarding	
#	The number of the item in this list.
Active	Select this to enable this rule. Clear this to disable this rule.
Name	This field displays the name of the rule. It does not have to be unique.
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the Start Port , only one port number is forwarded.
Server IP Address	This field displays the IP address of the server to which packet for the selected port(s) are forwarded.
Action	Click the Edit icon to set up a port forwarding rule or alter the configuration of an existing port forwarding rule. Click the Delete icon to remove an existing port forwarding rule.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

8.3.2 Port Forwarding Rule Setup

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

Figure 29 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

The following table describes the labels in this screen.

Table 27 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

LABEL	DESCRIPTION
Active	Select this to enable this rule. Clear this to disable this rule.
Service Name	Enter a name to identify this rule. You can use 1 - 31 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Start Port End Port	Enter the port number or range of port numbers you want to forward to the specified server. To forward one port number, enter the port number in the Start Port and End Port fields. To forward a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field.
Server IP Address	Enter the IP address of the server to which to forward packets for the selected port number(s). This server is usually on the LAN.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

8.4 Trigger Port

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 OX253P 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 OX253P's WAN port receives a response with a specific port number and protocol ("incoming" port), the OX253P 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.

Click **ADVANCED > NAT Configuration > Trigger Port** to maintain trigger port forwarding rules for the OX253P.

Figure 30 ADVANCED > NAT Configuration > Trigger Port

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
10	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
11	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
12	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

The following table describes the labels in this screen.

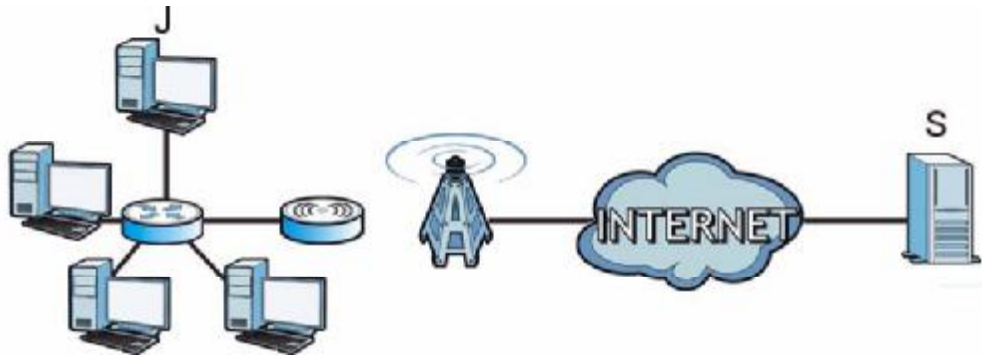
Table 28 ADVANCED > NAT Configuration > Trigger Port

LABEL	DESCRIPTION
#	The number of the item in this list.
Name	Enter a name to identify this rule. You can use 1 - 15 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Incoming	
Start Port End Port	<p>Enter the incoming port number or range of port numbers you want to forward to the IP address the OX253P records.</p> <p>To forward one port number, enter the port number in the Start Port and End Port fields.</p> <p>To forward a range of ports,</p> <ul style="list-style-type: none"> • enter the port number at the beginning of the range in the Start Port field • enter the port number at the end of the range in the End Port field. <p>If you want to delete this rule, enter zero in the Start Port and End Port fields.</p>
Trigger	
Start Port End Port	<p>Enter the outgoing port number or range of port numbers that makes the OX253P 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 Start Port and End Port fields.</p> <p>To select a range of ports,</p> <ul style="list-style-type: none"> • enter the port number at the beginning of the range in the Start Port field • enter the port number at the end of the range in the End Port field. <p>If you want to delete this rule, enter zero in the Start Port and End Port fields.</p>
Apply	Click to save your changes.
Reset	Click to return to the previous screen without saving your changes.

8.4.1 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 31 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 OX253P to record Jane's computer IP address. The OX253P 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 OX253P 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 OX253P 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 OX253P 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.

8.5 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.

Click **ADVANCED > NAT Configuration > ALG** to enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the OX253P.

Figure 32 ADVANCED > NAT Configuration > ALG

The screenshot shows a configuration window with a white background and a thin black border. On the left side, there are three lines of text, each preceded by a small green checkmark in a square box. The text reads: 'Enable SIP ALG', 'Enable FTP ALG', and 'Enable H.323 ALG'. Below these options, there is a horizontal line. At the bottom right of the window, there are two buttons: 'Apply' and 'Cancel', both with a light gray background and a thin black border.

The following table describes the labels in this screen.

Table 29 ADVANCED > NAT Configuration > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and port-triggering rules.
Enable FTP ALG	Select this to make sure FTP (file transfer) works correctly with port-forwarding and port-triggering rules.
Enable H.323 ALG	Select this to make sure H.323 (audio-visual programs, such as NetMeeting) works correctly with port-forwarding and port-triggering rules.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

The System Configuration Screens

9.1 Overview

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

9.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 9.2 on page 89](#)) lets you change the OX253P's mode, set up its system name, domain name, idle timeout, and administrator password.
- The **Dynamic DNS** screen ([Section 9.3 on page 90](#)) lets you set up the OX253P as a dynamic DNS client.
- The **Firmware** screen ([Section 9.4 on page 92](#)) lets you upload new firmware to the OX253P.
- The **Configuration** screen ([Section 9.5 on page 93](#)) lets you back up or restore the configuration of the OX253P.
- The **Restart** screen ([Section 9.6 on page 95](#)) lets you restart your OX253P from within the web configurator.

9.1.2 What You Need to Know

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

System Name

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

- In Windows 2000: Click **Start > Settings > Control Panel** and then double-click the **System** icon. Select the **Network Identification** tab and then click the **Properties** button. Note the entry for the **Computer Name** field and enter it as the **System Name**.

- In Windows XP: Click **Start > My Computer > View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the **OX253P System Name**.

Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the OX253P via DHCP.

DNS Server Address Assignment

Use DNS (Domain Name System) to map 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 computer before you can access it.

The OX253P can get the DNS server addresses in the following ways:

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

9.2 General

Click **ADVANCED > System Configuration > General** to change the OX253P's mode, set up its system name, domain name, idle timeout, and administrator password.

Figure 33 ADVANCED > System Configuration > General

The screenshot shows two sections of a configuration screen. The first section, titled "System Setup", contains three input fields: "System Name" with the value "OX253P", "Domain Name" which is empty, and "Administrator Inactivity Timer" with the value "5" and a note "(minutes, 0 means no timeout)". The second section, titled "Password Setup", contains three input fields: "Old Password", "New Password", and "Retype to Confirm", all of which are masked with asterisks. At the bottom right of the form are two buttons: "Apply" and "Reset".

The following table describes the labels in this screen.

Table 30 ADVANCED > System Configuration > General

LABEL	DESCRIPTION
System Setup	
System Name	Enter your computer's "Computer Name". This is for identification purposes, but some ISPs also check this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name entry that is propagated to DHCP clients on the LAN. If you leave this blank, the domain name obtained from the ISP is used. Use up to 38 alphanumeric characters. Spaces are not allowed, but dashes "-" and periods "." are accepted.
Administrator Inactivity Timer	Enter the number of minutes a management session can be left idle before the session times out. After it times out, you have to log in again. A value of "0" means a management session never times out, no matter how long it has been left idle. This is not recommended. Long idle timeouts may have security risks. The default is five minutes.
Password Setup	
Old Password	Enter the current password you use to access the OX253P.
New Password	Enter the new password for the OX253P. You can use up to 30 characters. As you type the password, the screen displays an asterisk (*) for each character you type.

Table 30 ADVANCED > System Configuration > General (continued)

LABEL	DESCRIPTION
Retype to Confirm	Enter the new password again.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

9.3 Dynamic DNS

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

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

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

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

Click **ADVANCED > System Configuration > Dynamic DNS** to set up the OX253P as a dynamic DNS client.

Figure 34 ADVANCED > System Configuration > Dynamic DNS

The following table describes the labels in this screen.

Table 31 ADVANCED > System Configuration > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Enable Dynamic DNS	Select this to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Enter the host name. You can specify up to two host names, separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select this to enable the DynDNS Wildcard feature.
Enable offline option	This field is available when CustomDNS is selected in the DDNS Type field. Select this if your Dynamic DNS service provider redirects traffic to a URL that you can specify while you are off line. Check with your Dynamic DNS service provider.

Table 31 ADVANCED > System Configuration > Dynamic DNS (continued)

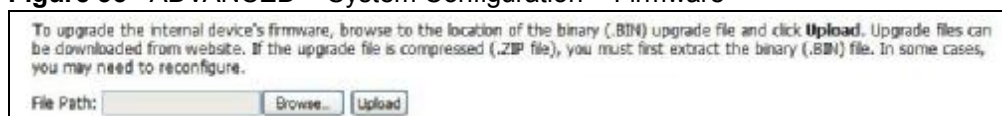
LABEL	DESCRIPTION
IP Address Update Policy	
Use WAN IP Address	Select this if you want the OX253P to update the domain name with the WAN port's IP address.
Dynamic DNS server auto detect IP address	Select this if you want the DDNS server to update the IP address of the host name(s) automatically. Select this option when there are one or more NAT routers between the OX253P and the DDNS server. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the OX253P and the DDNS server.
Use specified IP address	Select this if you want to use the specified IP address with the host name(s). Then, specify the IP address. Use this option if you have a static IP address.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

9.4 Firmware

Click **ADVANCED > System Configuration > Firmware** to upload new firmware to the OX253P. Firmware files usually use the system model name with a ".bin" extension, such as "OX253P.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Contact your service provider for information on available firmware upgrades.

Note: Only use firmware for your OX253P's specific model.

Figure 35 ADVANCED > System Configuration > Firmware

The following table describes the labels in this screen.

Table 32 ADVANCED > System Configuration > Firmware

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

Table 32 ADVANCED > System Configuration > Firmware (continued)

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

9.4.1 The Firmware Upload Process

When the OX253P uploads new firmware, the process usually takes about two minutes. The device also automatically restarts in this time. This causes a temporary network disconnect.

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

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

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

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

9.5 Configuration

Click **ADVANCED > System Configuration > Configuration** to back up or restore the configuration of the OX253P. You can also use this screen to reset the OX253P to the factory default settings.

Figure 36 ADVANCED > System Configuration > Configuration

Backup Configuration

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

Restore Configuration

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

File Path:

Back to Factory Defaults

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

- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

The following table describes the labels in this screen.

Table 33 ADVANCED > System Configuration > Configuration

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click this to save the OX253P's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.
Restore Configuration	
File Path	Enter the location of the file you want to upload, or click Browse... to find it.
Browse	Click this to find the file you want to upload.
Upload	Click this to restore the selected configuration file. Note: Do not turn off the device while configuration file upload is in progress.
Back to Factory Defaults	
Reset	Click this to clear all user-entered configuration information and return the OX253P to its factory defaults. There is no warning screen.

9.5.1 The Restore Configuration Process

When the OX253P 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 OX253P's IP address is different in the configuration file you selected, you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See the Quick Start Guide or the appendices for details on how to set up your computer's IP address.

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

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

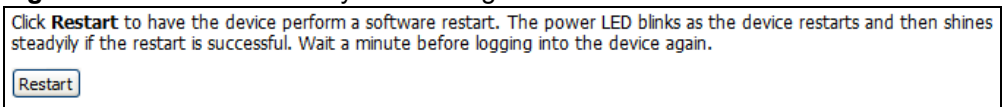
Click **Return** to go back to the **Configuration** screen.

9.6 Restart

Click **ADVANCED > System Configuration > Restart** to reboot the OX253P without turning the power off.

Note: Restarting the OX253P does not affect its configuration.

Figure 37 ADVANCED > System Configuration > Restart



The following table describes the labels in this screen.

Table 34 ADVANCED > System Configuration > Firmware

LABEL	DESCRIPTION
Restart	Click this button to have the device perform a software restart. The Power LED blinks as it restarts and the shines steadily if the restart is successful. Note: Wait one minute before logging back into the OX253P after a restart.

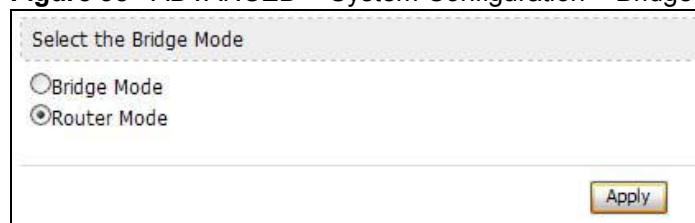
9.6.1 The Restart Process

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

9.7 Bridge

Click **ADVANCED > System Configuration > Bridge** to switch the OX253P between the bridge or router mode. You may need the bridge mode when you need to use VLAN applications in your network.

Figure 38 ADVANCED > System Configuration > Bridge



The following table describes the labels in this screen.

Table 35 ADVANCED > System Configuration > Bridge

LABEL	DESCRIPTION
Bridge Mode	Select this to switch to the bridge mode for the OX253P.
Router Mode	Select this to switch to the router mode for the OX253P.
Apply	Click to save your change.

The Certificates Screens

10.1 Overview

Use the **TOOLS > Certificates** screens to manage public key certificates on the OX253P.

The OX253P can use public key certificates (also sometimes called "digital IDs") to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

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

10.1.1 What You Can Do in This Chapter

- The **My Certificates** screen ([Section 10.2 on page 98](#)) lets you generate and export self-signed certificates or certification requests and import the OX253P's CA-signed certificates.
- The **Trusted CAs** screen ([Section 10.3 on page 108](#)) lets you display a summary list of certificates of the certification authorities that you have set the OX253P to accept as trusted.

10.1.2 What You Need to Know

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

Certificate Authorities

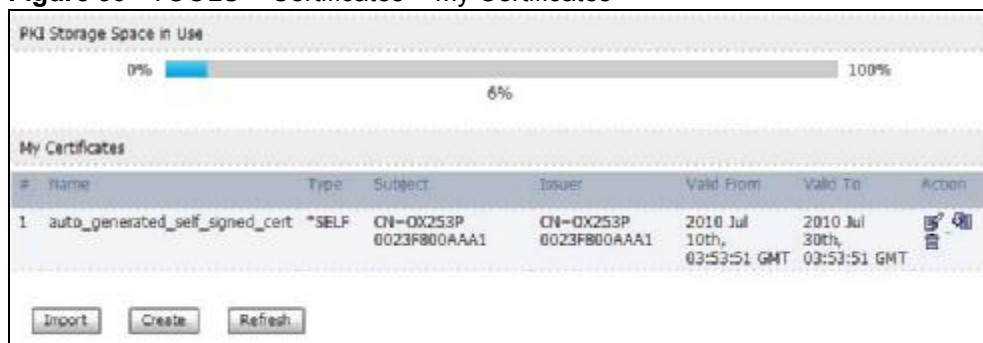
A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the

OX253P to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

10.2 My Certificates




Click **TOOLS > Certificates > My Certificates** to access this screen. Use this screen to generate and export self-signed certificates or certification requests and import the OX253P's CA-signed certificates.

Figure 39 TOOLS > Certificates > My Certificates



The following table describes the icons in this screen.

Table 36 TOOLS > Certificates > My Certificates

ICON	DESCRIPTION
	Edit Click to edit this item.
	Export Click to export an item.
	Delete Click to delete this item.

The following table describes the labels in this screen.

Table 37 TOOLS > Certificates > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the OX253P's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The number of the item in this list.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 37 TOOLS > Certificates > My Certificates (continued)

LABEL	DESCRIPTION
Type	<p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>*SELF represents the default self-signed certificate which signs the imported remote host certificates.</p> <p>CERT represents a certificate issued by a certification authority.</p>
Subject	<p>This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.</p>
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.</p>
Valid From	<p>This field displays the date that the certificate becomes applicable.</p>
Valid To	<p>This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.</p>
Action	<p>Click the Edit icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the Export icon to save a copy of the certificate without its private key. Browse to the location you want to use and click Save.</p> <p>Click the Delete icon to remove a certificate. A window displays asking you to confirm that you want to delete the certificate. Subsequent certificates move up by one when you take this action.</p> <p>The OX253P keeps all of your certificates unless you specifically delete them. Uploading new firmware or default configuration file does not delete your certificates.</p> <p>You cannot delete certificates that any of the OX253P's features are configured to use.</p>
Import	<p>Click to a certificate into the OX253P.</p>
Create	<p>Click to go to the screen where you can have the OX253P generate a certificate or a certification request.</p>
Refresh	<p>Click to display the current validity status of the certificates.</p>

10.2.1 My Certificates Create

Click **TOOLS > Certificates > My Certificates** and then the **Create** icon to open the **My Certificates Create** screen. Use this screen to have the OX253P create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 40 TOOLS > Certificates > My Certificates > Create

The screenshot displays the 'My Certificates Create' interface. At the top, there is a text input field for 'Certificate Name:'. Below this is a section titled 'Subject Information' with a dashed border. It contains several fields: 'Common Name:' with radio buttons for 'Host IP Address:' (selected), 'Host Domain Name:', and 'E-Mail:'. The 'Host IP Address:' field is pre-filled with '0 . 0 . 0 . 0'. Other fields include 'Organizational Unit:', 'Organization:', and 'Country:'. A 'Key Length:' dropdown menu is set to '512'. The next section is 'Enrollment Options', also with a dashed border. It features three radio buttons: 'Create a self-signed certificate' (selected), 'Create a certification request and save it locally for later manual enrollment', and 'Create a certification request and enroll for a certificate immediately online'. Below these are 'Enrollment Protocol:' (set to 'Simple Certificate Enrollment Protocol (SCEP)'), 'CA Server Address:', 'CA Certificate:' (with a dropdown arrow and a link to 'Trusted CAs'), and 'Request Authentication'. A 'Key:' field is at the bottom. 'Apply' and 'Cancel' buttons are located in the bottom right corner.

The following table describes the labels in this screen.

Table 38 TOOLS > Certificates > My Certificates > Create

LABEL	DESCRIPTION
Certificate Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;`~!@#\$%^&()_+[]{}',.- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the Common Name is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	<p>Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string.</p> <p>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.</p> <p>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.</p>
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 63 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 63 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the state in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select Create a self-signed certificate to have the OX253P generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	<p>Select Create a certification request and save it locally for later manual enrollment to have the OX253P generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority.</p> <p>Copy the certification request from the My Certificate Details screen and then send it to the certification authority.</p>

Table 38 TOOLS > Certificates > My Certificates > Create

LABEL	DESCRIPTION
Create a certification request and enroll for a certificate immediately online	<p>Select Create a certification request and enroll for a certificate immediately online to have the OX253P generate a request for a certificate and apply to a certification authority for a certificate.</p> <p>You must have the certification authority's certificate already imported in the Trusted CAs screen.</p> <p>When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.</p>
Enrollment Protocol	<p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Select the certification authority's enrollment protocol from the drop-down list box.</p> <p>Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.</p> <p>Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.</p>
CA Server Address	<p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Enter the IP address (or URL) of the certification authority server.</p> <p>For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@\$_%&-</p>
CA Certificate	<p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Select the certification authority's certificate from the CA Certificate drop-down list box.</p> <p>You must have the certification authority's certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the OX253P's list of certificates of trusted certification authorities.</p>
Request Authentication	<p>When you select Create a certification request and enroll for a certificate immediately online, the certification authority may want you to include a reference number and key to identify you when you send a certification request.</p> <p>Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just the Key field displays if your certification authority uses the SCEP enrollment protocol.</p> <p>For the reference number, use 0 to 999999999.</p> <p>For the key, use up to 31 of the following characters. a-zA-Z0-9; `~!@#\$\$%^&*()_+\\{}':./<>=-</p>

Table 38 TOOLS > Certificates > My Certificates > Create

LABEL	DESCRIPTION
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

If you configured the **My Certificate Create** screen to have the OX253P enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the OX253P to enroll a certificate online.

10.2.2 My Certificate Edit

Click **TOOLS > Certificates > My Certificates** then the **Edit** icon to access this screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 41 TOOLS > Certificates > My Certificates > Edit

The following table describes the labels in this screen.

Table 39 TOOLS > Certificates > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;`~!@#\$\$%^&()_+[]{}',.- characters.
Property	Select Default self-signed certificate which signs the imported remote host certificates to use this certificate to sign the remote host certificates you upload in the TOOLS > Certificates > Trusted CAs screen.

Table 39 TOOLS > Certificates > My Certificates > Edit

LABEL	DESCRIPTION
Certification Path	<p>This field displays for a certificate, not a certification request.</p> <p>Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).</p> <p>If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The OX253P does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.</p>
Refresh	Click to display the certification path.
Certification Information	
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number. "
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the OX253P.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.</p> <p>With self-signed certificates, this is the same as the Subject Name field.</p> <p>"none" displays for a certification request.</p>
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The OX253P uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the OX253P uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).

Table 39 TOOLS > Certificates > My Certificates > Edit

LABEL	DESCRIPTION
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the OX253P calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the OX253P calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

10.2.3 My Certificate Import

Click **TOOLS > Certificates > My Certificates > Import** to access this screen. Use this screen to import a certificate that matches a corresponding certification request that was generated by the OX253P. You must remove any spaces from the certificate's filename before you can import it.

Figure 42 TOOLS > Certificates > My Certificates > Import

The following table describes the labels in this screen.

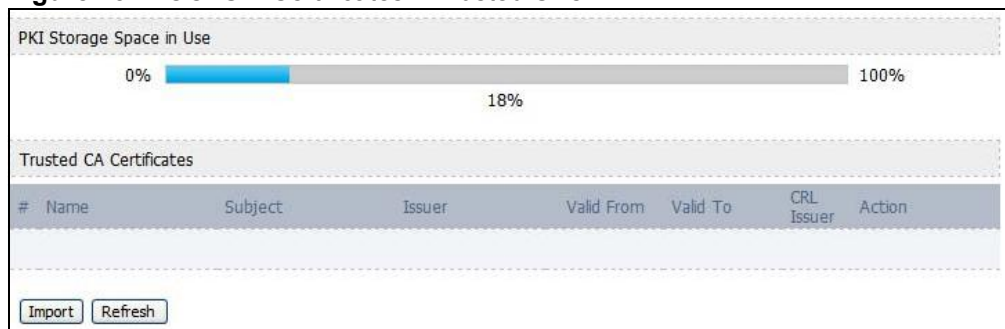
Table 40 TOOLS > Certificates > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the OX253P.
Browse	Click to find the certificate file you want to upload.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

10.3 Trusted CAs




Click **TOOLS > Certificates > Trusted CAs** access this screen. Use this screen to display a summary list of certificates of the certification authorities that you have set the OX253P to accept as trusted. The OX253P accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 43 TOOLS > Certificates > Trusted CAs



The following table describes the icons in this screen.

Table 41 TOOLS > Certificates > Trusted CAs

ICON	DESCRIPTION
	Edit Click to edit this item.
	Export Click to export an item.
	Delete Click to delete this item.

The following table describes the labels in this screen.

Table 42 TOOLS > Certificates > Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the OX253P's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The number of the item in this list.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

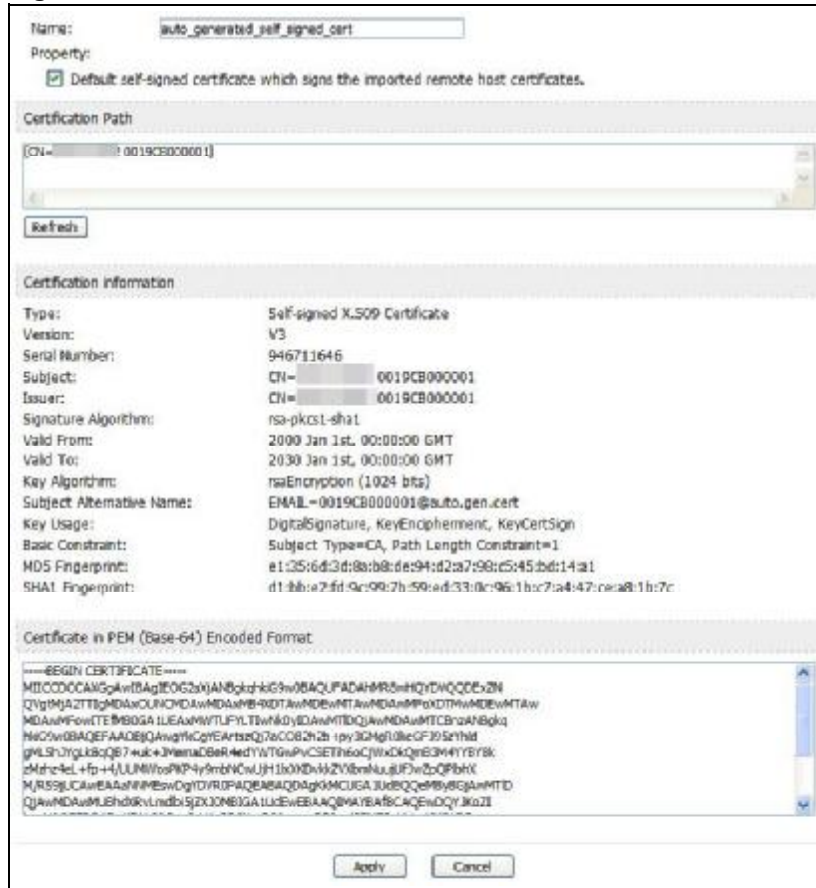
Table 42 TOOLS > Certificates > Trusted CAs (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues CRL (Certificate Revocation Lists) for the certificates that it has issued and you have selected the Check incoming certificates issued by this CA against a CRL check box in the certificate's details screen to have the OX253P check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays No .
Action	<p>Click the Edit icon to open a screen with an in-depth list of information about the certificate.</p> <p>Use the Export icon to save the certificate to a computer. Click the icon and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.</p> <p>Click the Delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.</p>
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the OX253P.
Refresh	Click this button to display the current validity status of the certificates.

10.3.1 Trusted CA Edit

Click **TOOLS > Certificates > Trusted CAs** and then click the **Edit** icon to open the **Trusted CAs** screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 44 TOOLS > Certificates > Trusted CAs > Edit



The following table describes the labels in this screen.

Table 43 TOOLS > Certificates > Trusted CAs > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;`~!@#\$\$%^&()_+[]{}',.- characters.
Property	Select Default self-signed certificate which signs the imported remote host certificates to use this certificate to sign the remote host certificates you upload in the TOOLS > Certificates > Trusted CAs screen.

Table 43 TOOLS > Certificates > Trusted CAs > Edit (continued)

LABEL	DESCRIPTION
Certification Path	<p>This field displays for a certificate, not a certification request.</p> <p>Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).</p> <p>If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The OX253P does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.</p>
Refresh	Click Refresh to display the certification path.
Certification Information	
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number. "
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the OX253P.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.</p> <p>With self-signed certificates, this is the same as the Subject Name field.</p> <p>"none" displays for a certification request.</p>
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The OX253P uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the OX253P uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).

Table 43 TOOLS > Certificates > Trusted CAs > Edit (continued)

LABEL	DESCRIPTION
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the OX253P calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the OX253P calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

10.3.2 Trusted CA Import

Click **TOOLS > Certificates > Trusted CAs** and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate from a computer to the OX253P. The OX253P trusts any valid certificate signed by any of the imported trusted CA certificates.

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

Figure 45 TOOLS > Certificates > Trusted CAs > Import

The following table describes the labels in this screen.

Table 44 TOOLS > Certificates > Trusted CAs Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Choose...	Click to find the certificate file you want to upload.
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

10.4 Technical Reference

The following section contains additional technical information about the OX253P features described in this chapter.

10.4.1 Certificate Authorities

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

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

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

The OX253P uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

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

A certification path is the hierarchy of certification authority certificates that validate a certificate. The OX253P does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the

scheduled expiration is called a CRL (Certificate Revocation List). The OX253P can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

10.4.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The OX253P only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

10.4.1.2 Self-signed Certificates

You can have the OX253P act as a certification authority and sign its own certificates.

10.4.1.3 Factory Default Certificate

The OX253P generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

10.4.1.4 Certificate File Formats

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

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The OX253P currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

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

10.4.2 Verifying a Certificate

Before you import a certificate into the OX253P, you should verify that you have the correct certificate. This is especially true of trusted certificates since the OX253P also trusts any valid certificate signed by any of the imported trusted certificates.

10.4.2.1 Checking the Fingerprint of a Certificate on Your Computer

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

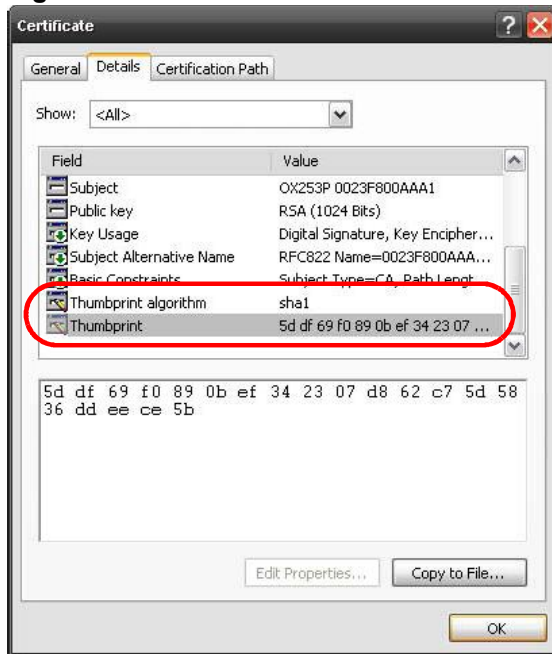
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension. (On some Linux distributions, the file extension may be ".der".) Add the file name extension manually if the file does not have any.

Figure 46 Remote Host Certificates



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

Figure 47 Certificate Details



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

The Firewall Screens

11.1 Overview

Use the **TOOLS > Firewall** screens to manage OX253P's firewall security measures.

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

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

11.1.1 What You Can Do in This Chapter

- The **Firewall Setting** screen ([Section 11.2 on page 120](#)) lets you configure the basic settings for your firewall.
- The **Service Setting** screen ([Section 11.3 on page 123](#)) lets you enable service blocking, set up the date and time service blocking is effective, and to maintain the list of services you want to block.

11.1.2 What You Need to Know

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

About the OX253P Firewall

The OX253P firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The OX253P's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet.

The OX253P can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The OX253P 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.

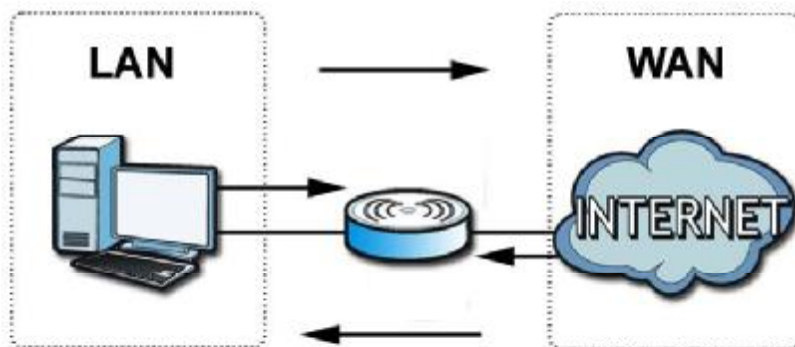
The OX253P has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

11.2 Firewall Setting

This section describes firewalls and the built-in OX253P's firewall features.

11.2.1 Firewall Rule Directions

Figure 48 Firewall Rule Directions



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

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

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

LAN-to-LAN/OX253P means the LAN to the OX253P LAN interface. This is always allowed, as this is how you manage the OX253P from your local computer.

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

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

- Configuring NAT port forwarding rules.
- Configuring WAN or LAN & WAN access for services in the Remote MGMT screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/OX253P firewall rules. WAN-to-WAN/OX253P firewall rules are Internet to the OX253P WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what WAN-to-LAN and WAN-to-WAN/OX253P packets to log.

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

11.2.2 Triangle Route

When the firewall is on, your OX253P acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the OX253P to protect your LAN against attacks.

Figure 49 Ideal Firewall Setup



11.2.3 Firewall Setting Options

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

Figure 50 TOOLS > Firewall > General

Enable Firewall (Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.)
 Bypass Triangle Route
 Max NAT/Firewall Session Per User:

Packet Direction: Log
 LAN to WAN:
 WAN to LAN:

The following table describes the labels in this screen.

Table 45 TOOLS > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this to activate the firewall. The OX253P controls access and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this if you want to let some traffic from the WAN go directly to a computer in the LAN without passing through the OX253P.
Max NAT/ Firewall Session Per User	Select the maximum number of NAT rules and firewall rules the OX253P enforces at one time. The OX253P automatically allocates memory for the maximum number of rules, regardless of whether or not there is a rule to enforce. This is the same number you enter in ADVANCED > NAT Configuration > General .
Packet Direction	
Log	Select the situations in which you want to create log entries for firewall events. No Log - do not create any log entries Log Blocked - (LAN to WAN only) create log entries when packets are blocked Log Forwarded - (WAN to LAN only) create log entries when packets are forwarded Log All - create log entries for every packet
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

11.3 Services

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

Figure 51 TOOLS > Firewall > Services

The following table describes the labels in this screen.

Table 46 TOOLS > Firewall > Services

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

Table 46 TOOLS > Firewall > Services (continued)

LABEL	DESCRIPTION
Available Services	This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click Add to add the port to the Blocked Services field. A custom port is a service that is not available in the pre-defined Available Services list. You must define it using the Type and Port Number fields.
Blocked Services	This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click Delete .
Type	Select TCP or UDP , based on which one the custom port uses.
Port Number	Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range of 6345-6349 .
Add	Click this to add the selected service in Available Services to the Blocked Services list.
Delete	Select a service in the Blocked Services , and click this to remove the service from the list.
Clear All	Click this to remove all the services in the Blocked Services list.
Schedule to Block	
Day to Block	Select which days of the week you want the service blocking to be effective.
Time of Day to Block	Select what time each day you want service blocking to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

11.4 Technical Reference

The following section contains additional technical information about the OX253P features described in this chapter.

11.4.1 Stateful Inspection Firewall.

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

11.4.2 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via web configurator.
- 2 Think about access control before you connect to the network in any way.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

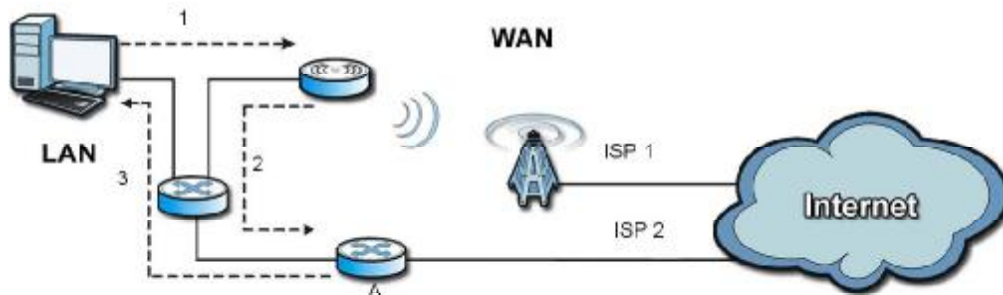
11.4.3 The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the OX253P's LAN IP address), the “triangle route” (also called asymmetrical route) problem may occur. The steps below describe the “triangle route” problem.

- 1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2 The OX253P reroutes the SYN packet through Gateway A on the LAN to the WAN.
- 3 The reply from the WAN goes directly to the computer on the LAN without going through the OX253P.

As a result, the OX253P resets the connection, as the connection has not been acknowledged.

Figure 52 “Triangle Route” Problem



11.4.3.1 Solving the “Triangle Route” Problem

If you have the OX253P allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the OX253P and its firewall protection.

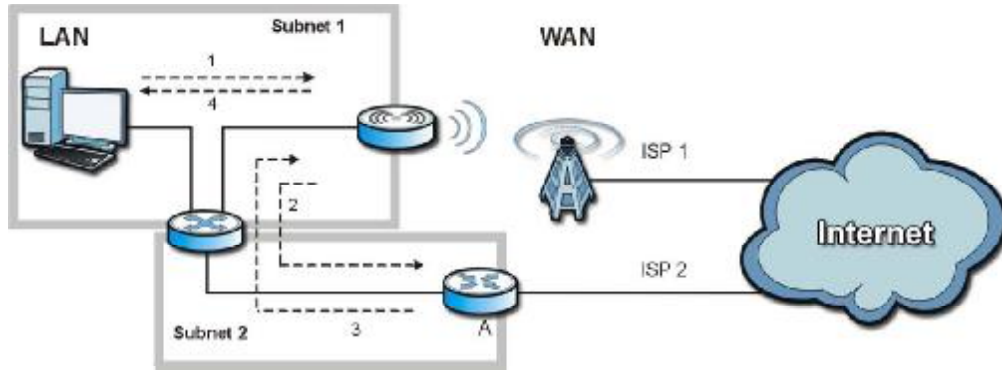
Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your OX253P supports up to three logical LAN interfaces with the OX253P being the gateway for each logical network.

It's like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway A in different subnets, all returning network traffic must pass through the OX253P to your LAN. The following steps describe such a scenario.

- 1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The OX253P reroutes the packet to Gateway A, which is in Subnet 2.
- 3 The reply from the WAN goes to the OX253P.

- The OX253P then sends it to the computer on the LAN in Subnet 1.

Figure 53 IP Alias



Content Filter

12.1 Overview

Use the **TOOLS > Content Filter** screens to create and enforce policies that restrict access to the Internet based on content

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords. The OX253P can block web features such as ActiveX controls, Java applets, cookies and disable web proxies. The OX253P also allows you to define time periods and days during which the OX253P performs content filtering.

12.1.1 What You Can Do in This Chapter

- The **Filter** screen ([Section 12.2 on page 130](#)) lets you set up a trusted IP address, which web features are restricted, and which keywords are blocked when content filtering is effective.
- The **Schedule** screen ([Section 12.3 on page 132](#)) lets you schedule content filtering.

12.2 Filter

Click **TOOLS > Content Filter > Filter** to set up a trusted IP address, which web features are restricted, and which keywords are blocked when content filtering is effective.

Figure 54 TOOLS > Content Filter > Filter

The screenshot shows the 'Filter' configuration page with the following sections:

- Trusted IP Setup**: A text box for 'Trusted Computer IP Address' containing '0.0.0.0'. A note states: 'A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.'
- Restrict Web Features**: Four unchecked checkboxes for 'ActiveX', 'Java', 'Cookies', and 'Web Proxy'.
- Keyword Blocking**: A checked checkbox for 'Enable URL Keyword Blocking'. Below it is a 'Keyword:' text box and an 'Add' button.
- Keyword List**: A text area containing 'spam' and 'wankle%20rotary%20engine'. Below it are 'Delete' and 'Clear All' buttons.
- Message to display when a site is blocked**: A text box for 'Denied Access Message:'.
- At the bottom are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 47 TOOLS > Content Filter > Filter

LABEL	DESCRIPTION
Trusted IP Setup	
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without the restrictions you set in these screens. Enter the IP address of the trusted computer.
Restrict Web Features	Select the web features you want to disable. If a user downloads a page with a restricted feature, that part of the web page appears blank or grayed out. ActiveX - This is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. Java - This is used to build downloadable Web components or Internet and intranet business applications of all kinds. Cookies - This is used by Web servers to track usage and to provide service based on ID. Web Proxy - This is a server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to avoid content filtering restrictions.
Keyword Blocking	
Enable URL Keyword Blocking	Select this if you want the OX253P to block Web sites based on words in the web site address. For example, if you block the keyword bad, http://www.website.com/bad.html is blocked.
Keyword	Type a keyword you want to block in this field. You can use up to 128 printable ASCII characters. There is no wildcard character, however.
Add	Click this to add the specified Keyword to the Keyword List . You can enter up to 128 keywords.
Keyword List	This field displays the keywords that are blocked when Enable URL Keyword Blocking is selected. To delete a keyword, select it, click Delete , and click Apply .
Delete	Click Delete to remove the selected keyword in the Keyword List . The keyword disappears after you click Apply .
Clear All	Click this button to remove all of the keywords in the Keyword List .
Denied Access Message	Enter the message that is displayed when the OX253P's content filter feature blocks access to a web site.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

12.3 Schedule

Click **TOOLS > Content Filter > Schedule** to schedule content filtering.

Figure 55 TOOLS > Content Filter > Schedule

Day to Block:

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Block: (24-Hour Format)

All day

From: Start (hour) (min) End (hour) (min)

The following table describes the labels in this screen.

Table 48 TOOLS > Content Filter > Schedule

LABEL	DESCRIPTION
Day to Block	Select which days of the week you want content filtering to be effective.
Time of Day to Block	Select what time each day you want content filtering to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

The Remote Management Screens

13.1 Overview

Use the **TOOLS > Remote Management** screens to control which computers can use which services to access the OX253P on each interface.

Remote management allows you to determine which services/protocols can access which OX253P interface (if any) from which computers.

You may manage your OX253P from a remote location via:

Table 49 Remote Management

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

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

You may only have one remote management session running at a time. The OX253P automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Telnet
- 2 HTTP

13.1.1 What You Can Do in This Chapter

- The **WWW** screen ([Section 13.2 on page 135](#)) lets you control HTTP access to your OX253P.
- The **Telnet** screen ([Section 13.3 on page 136](#)) lets you control Telnet access to your OX253P.
- The **FTP** screen ([Section 13.4 on page 136](#)) lets you control FTP access to your OX253P.

- The **SNMP** screen ([Section 13.5 on page 137](#)) lets you control SNMP access to your OX253P.
- The **DNS** screen ([Section 13.6 on page 140](#)) lets you control DNS access to your OX253P.
- The **Security** screen ([Section 13.7 on page 141](#)) lets you control how your OX253P responds to other types of requests.
- The **CWMP-TR069** screen ([Section 13.8 on page 142](#)) lets you configure the OX253P's auto-configuration and dynamic service configuration options.

13.1.2 What You Need to Know

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

Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the OX253P will disconnect the session immediately.
- 4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

Remote Management and NAT

When NAT is enabled:

- Use the OX253P's WAN IP address when configuring from the WAN.
- Use the OX253P's LAN IP address when configuring from the LAN.

System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The OX253P 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. You can change the timeout period in the **Maintenance > System > General** screen.

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 OX253P supports SNMP agent functionality, which allows a manager station to manage and monitor the OX253P through the network. The OX253P 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.

13.2 WWW

Click **TOOLS > Remote Management > WWW** to control HTTP access to your OX253P.

Figure 56 TOOLS > Remote Management > WWW

The following table describes the labels in this screen.

Table 50 TOOLS > Remote Management > WWW

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the OX253P. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the OX253P using this service.
Secured Client IP Address	Select All to allow any computer to access the OX253P using this service. Select Selected to only allow the computer with the IP address that you specify to access the OX253P using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

13.3 Telnet

Click **TOOLS > Remote Management > Telnet** to control Telnet access to your OX253P.

Figure 57 TOOLS > Remote Management > Telnet

The following table describes the labels in this screen.

Table 51 TOOLS > Remote Management > Telnet

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the OX253P. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the OX253P using this service.
Secured Client IP Address	Select All to allow any computer to access the OX253P using this service. Select Selected to only allow the computer with the IP address that you specify to access the OX253P using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

13.4 FTP

Click **TOOLS > Remote Management > FTP** to control FTP access to your OX253P.

Figure 58 TOOLS > Remote Management > FTP

The following table describes the labels in this screen.

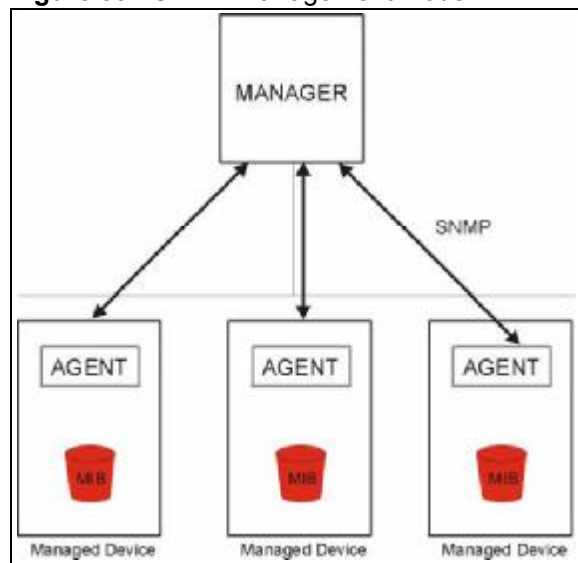
Table 52 TOOLS > Remote Management > FTP

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the OX253P. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the OX253P using this service.
Secured Client IP Address	Select All to allow any computer to access the OX253P using this service. Select Selected to only allow the computer with the IP address that you specify to access the OX253P using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

13.5 SNMP

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

Figure 59 SNMP Management Model



An agent is a management software module that resides in a managed device (the OX253P). 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 OX253P 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.

13.5.1 SNMP Traps

The OX253P sends traps to the SNMP manager when any of the following events occurs:

Table 53 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	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.

13.5.2 SNMP Options

Click **TOOLS > Remote Management > SNMP** to access this screen. Use SNMP options to control SNMP access to your OX253P.

Figure 60 TOOLS > Remote Management > SNMP

The following table describes the labels in this screen.

Table 54 TOOLS > Remote Management > SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Enter the IP address of the station to send your SNMP traps to.
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the OX253P using this service.

Table 54 TOOLS > Remote Management > SNMP (continued)

LABEL	DESCRIPTION
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the OX253P using this service. Select All to allow any computer to access the OX253P using this service. Choose Selected to just allow the computer with the IP address that you specify to access the OX253P using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

13.6 DNS

Click **TOOLS > Remote Management > DNS** to access this screen. Use this screen to control DNS access to your OX253P.

Figure 61 TOOLS > Remote Management > DNS

The following table describes the labels in this screen.

Table 55 TOOLS > Remote Management > DNS

LABEL	DESCRIPTION
Server Port	This field is read-only. This field displays the port number this service uses to access the OX253P. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the OX253P using this service.
Secured Client IP Address	Select All to allow any computer to access the OX253P using this service. Select Selected to only allow the computer with the IP address that you specify to access the OX253P using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

13.7 Security

Click **TOOLS > Remote Management > Security** to access this screen. Use this screen to control how your OX253P responds to other types of requests.

Figure 62 TOOLS > Remote Management > Security

The following table describes the labels in this screen.

Table 56 TOOLS > Remote Management > Security

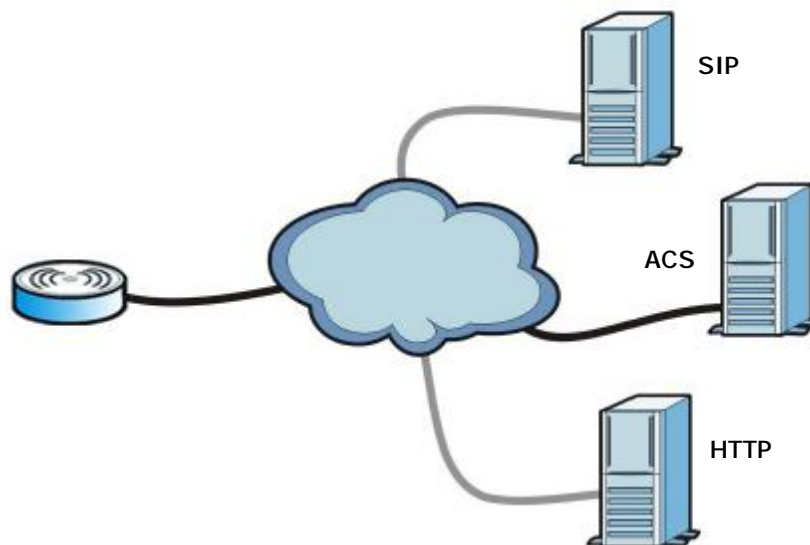
LABEL	DESCRIPTION
Respond to Ping on	<p>Select the interface(s) on which the OX253P should respond to incoming ping requests.</p> <ul style="list-style-type: none"> • Disable - the OX253P does not respond to any ping requests. • LAN - the OX253P only responds to ping requests received from the LAN. • WAN - the OX253P only responds to ping requests received from the WAN. • LAN & WAN - the OX253P responds to ping requests received from the LAN or the WAN.
Do not respond to requests for unauthorized services	<p>Select this to prevent outsiders from discovering your OX253P by sending requests to unsupported port numbers. If an outside user attempts to probe an unsupported port on your OX253P, an ICMP response packet is automatically returned. This allows the outside user to know the OX253P exists. Your OX253P supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your OX253P when unsupported ports are probed.</p> <p>If you clear this, your OX253P replies with an ICMP Port Unreachable packet for a port probe on unused UDP ports and with a TCP Reset packet for a port probe on unused TCP ports.</p>
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

13.8 CWMP-TR069

CWMP-TR069 is an abbreviation of "CPE WAN Management Protocol - Technical Reference 069", a protocol designed to facilitate the remote management of Customer Premise Equipment (CPE), such as the OX253P. It can be managed over a WAN by means of an Auto Configuration Server (ACS). CWMP-TR069 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 OX253P, modify its settings, perform firmware upgrades, and monitor and diagnose it. In order to do so, you must enable the CWMP-TR069 feature on your OX253P and then configure it appropriately. (The ACS server which it will use must also be configured by its administrator.)

Figure 63 CWMP-TR069 Example



In this example, the OX253P 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 OX253P remotely. All three servers are owned and operated by the client's Internet Service Provider. However, without the configuration settings from the ACS, the OX253P cannot access the other two servers. Once the OX253P 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 OX253P can be configured to periodically check for updates from the auto-configuration server so that the end user need not be worried about it.

Click **TOOLS > Remote Management > CWMP-TR069** to access this screen. Use this screen to open OX253P's auto-configuration and dynamic service configuration options.

Figure 64 TOOLS > Remote Management > CWMP-TR069

<input type="checkbox"/> Active	
ACS URL:	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Connection Request User Name:	<input type="text"/>
Connection Request Password:	<input type="text"/>
<input type="checkbox"/> Upgrade Managed	
<input type="checkbox"/> Periodic Inform Enable	
Periodic Inform Interval:	<input type="text" value="30"/> sec(Range:30~2147483647)
Periodic Inform Time(yyyy-mm-ddThh:mm:ss):	<input type="text" value="0000-00-00T00:00:00"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The following table describes the labels in this screen.

Table 57 TOOLS > Remote Management > CWMP-TR069

LABEL	DESCRIPTION
Active	Select this option to turn on the OX253P's CWMP-TR069 feature. Note: If this feature is not enabled then the OX253P cannot be managed remotely.
ACS URL	Enter the URL or IP address of the auto-configuration server.
User Name	Enter the user name sent when the OX253P 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.
Password	Enter the password sent when the OX253P 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.
Connection Request User Name	Enter the connection request user name that the ACS must send to the OX253P 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. Note: This must be provided by the ACS administrator.

Table 57 TOOLS > Remote Management > CWMP-TR069

LABEL	DESCRIPTION
Connection Request Password	<p>Enter the connection request password that the ACS must send to the OX253P when it requests a connection.</p> <p>You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.</p> <p>Note: This must be provided by the ACS administrator.</p>
Periodic Inform Enable	<p>Select this to allow the OX253P to periodically connect to the ACS and check for configuration updates.</p> <p>If you do not enable this feature then the OX253P can only be updated automatically when the ACS initiates contact with it and if you selected the Active checkbox on this screen.</p>
Periodic Inform Interval	<p>Enter the time interval (in seconds) at which the OX253P connects to the auto-configuration server.</p>
Periodic Inform Time	<p>Enter a time interval that the OX253P will trigger a periodic inform interval. This works in tandem with the Periodic Inform Interval and is not mutually exclusive of it.</p> <p>The Periodic Inform Time must be in the following format: yyyy-mm-ddThh:mm:ss where yyyy is a four digit year ("2009"), mm is a two digit month (01~12), dd is a two digit day (01~28), hh is a two-digit hour in 24-hour format (01~24), mm is a two digit minutes value (01-60) and ss is a two digit seconds value (01-60).</p> <p>Note: You must separate the day information from the hour information with a "T".</p> <p>This feature gives the OX253P a baseline from which to begin calculating when each periodic inform happens.</p> <p>If the inform time is set for some point in the past, the OX253P interpolates the inform interval forward to the current time and begins its periodic inform at the appropriate time based on this interpolation.</p> <p>If the inform time is set for some point in the future, then the OX253P interpolates backwards to the current time and actually begins at the appropriate time based on this interpolation.</p>
Apply	<p>Click to save your changes.</p>
Reset	<p>Click to restore your previously saved settings.</p>

14

QoS

14.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

14.2 General

Click **TOOLS > QoS** to open the screen as shown next. Use this screen to enable or disable QoS.

Figure 65 QoS > General



The following table describes the labels in this screen.

Table 58 TOOLS > Remote Management > Security

LABEL	DESCRIPTION
Active QoS	Select this to enable QoS for the OX253P. Selecting this may improve network performance, especially if you are using VoIP applications or are playing online video games.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

14.3 Class Setup

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the OX253P forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **TOOLS > QoS > Class Setup** to open the following screen.

Figure 66 QoS > Class Setup

#	Active	Name	Interface	DSCP	Class Index	Action
1		Default Class	To LAN	0	99	
2		Default Class	To WAN	0	99	

The following table describes the labels in this screen.

Table 59 QoS Class Setup

LABEL	DESCRIPTION
Create New Class	Click this link to create a new class.
#	This field displays the index number of the class.
Active	This field indicates whether the QoS class is enabled or not.
Name	This field indicates the name of the class.
Interface	This field indicates the Ethernet port on which traffic is being monitored and prioritized.
DSCP	This field indicates the Differentiated Services Code Point (DSCP) value for the associated class.
Class Index	This field indicates the index for this QoS class. Classes are implemented based on index number, from lowest to highest.
Action	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Apply	Click this button to save your changes back to the OX253P.
Cancel	Click this button to begin configuring this screen afresh.

14.3.1 Class Configuration

Click the **Create New Class** link or the edit icon next to a non-default class entry in the **Class Setup** screen to configure a classifier.

Figure 67 QoS > Class Setup > Create New Class

The following table describes the labels in this screen.

Table 60 Create New Class

LABEL	DESCRIPTION
Class Configuration	
Active	Select this to make a class active.
Index	Enter an index number for the class. Similar classes are processed in order of index number, from lowest to highest.
Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Interface	Select an interface to which the class will apply: <ul style="list-style-type: none"> To WAN - The class is applied to all packets incoming from the WAN (Wide Area Network). To LAN - The class is applied to all packets outgoing from the LAN (Local Area Network).
DSCP	Enter the Differentiated Services Code Point (DSCP) value (0~63) for the traffic matching the class criteria. The higher the value, the higher the priority. Lower-priority packets may be dropped if the total traffic exceeds the capacity of the network.

Table 60 Create New Class (continued)

LABEL	DESCRIPTION
Filter Configuration Use this section to define traffic to which this class will apply. The logical relationship of the following parameters is "AND". Select Exclude next to a parameter to not apply the class to the traffic matching the criteria.	
Source	
Address Subnet Mask	Enter a source IP address and the subnet mask for the criteria.
Port Range	Enter a port range on the source host for the criteria.
Destination	
Address Subnet Mask	Enter a destination IP address and the subnet mask for the criteria.
Port Range	Enter a port range on the destination host for the criteria.
Others	
Service	Select the traffic type of a service (SIP , FTP or H.323) to which this class will apply.
Protocol	Select TCP or UDP to specify the traffic type to which the class will apply. You can also select User Defined and enter the number of a protocol.
Apply	Click this button to save your changes back to the OX253P.
Cancel	Click this button to begin configuring this screen afresh.

The Logs Screens

15.1 Overview

Use the **TOOLS > Logs** screens to look at log entries and alerts and to configure the OX253P's log and alert settings.

For a list of log messages, see [Section 15.4 on page 155](#).

15.1.1 What You Can Do in This Chapter

- The **View Logs** screen ([Section 15.2 on page 151](#)) lets you look at log entries and alerts.
- The **Log Settings** screen ([Section 15.3 on page 153](#)) lets you configure where the OX253P sends logs and alerts, the schedule for sending logs, and which logs and alerts are sent or recorded.

15.1.2 What You Need to Know

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

Alerts

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts.

Syslog Logs

There are two types of syslog: event logs and traffic logs.

The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated.

A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer

can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 61 Syslog Logs

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the Log Settings screen. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DEV" for example).

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 62 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

15.2 View Logs

Click **TOOLS > Logs > View Log** to access this screen. Use this screen to look at log entries and alerts. Alerts are written in red.

Figure 68 TOOLS > Logs > View Logs

#	Time	Message	Source	Destination	Note
1	07/08/2008 05:09:30	Successful HTTP login	192.168.1.34		User:admin
2	07/08/2008 02:15:39	Successful HTTP login	192.168.1.34		User:admin
3	07/08/2008 02:09:00	Successful HTTP login	192.168.1.34		User:admin
4	07/08/2008 01:57:20	Successful HTTP login	192.168.1.34		User:admin
5	07/08/2008 01:34:07	Successful HTTP login	192.168.1.34		User:admin
6	07/08/2008 01:10:45	Successful HTTP login	192.168.1.34		User:admin
7	07/08/2008 00:49:27	Successful HTTP login	192.168.1.34		User:admin
8	07/08/2008 00:08:10	Successful HTTP login	192.168.1.34		User:admin
9	07/08/2008 00:07:37	DHCP server assigns 192.168.1.33 to TWPC13435-XP			
10	07/08/2008 00:07:37				
11	07/08/2008 00:07:34	DHCP server assigns 192.168.1.33 to TWPC13435-XP			
12	07/08/2008 00:07:34				
13	07/08/2008 00:07:34				
14	07/08/2008 00:05:14				

Click a column header to sort log entries in descending (later-to-earlier) order. Click again to sort in ascending order. The small triangle next to a column header indicates how the table is currently sorted (pointing downward is descending; pointing upward is ascending).

The following table describes the labels in this screen.

Table 63 TOOLS > Logs > View Logs

LABEL	DESCRIPTION
Display	Select a category whose log entries you want to view. To view all logs, select All Logs . The list of categories depends on what log categories are selected in the Log Settings page.
Email Log Now	Click this to send the log screen to the e-mail address specified in the Log Settings page.
Refresh	Click to renew the log screen.
Clear Log	Click to clear all the log entries, regardless of what is shown on the log screen.

Table 63 TOOLS > Logs > View Logs (continued)

LABEL	DESCRIPTION
#	The number of the item in this list.
Time	This field displays the time the log entry was recorded.
Message	This field displays the reason for the log entry. See Section 15.4 on page 155 .
Source	This field displays the source IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available.
Destination	This field lists the destination IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available.
Note	This field displays additional information about the log entry.

15.3 Log Settings

Click **TOOLS > Logs > Log Settings** to configure where the OX253P sends logs and alerts, the schedule for sending logs, and which logs and alerts are sent or recorded.

Figure 69 TOOLS > Logs > Log Settings

E-mail Log Settings

Mail Server: (Outgoing SMTP Server NAME or IP Address)

Mail Subject:

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Log Schedule: ▾

Day for Sending Log: ▾

Time for Sending Log: (hour) (minute)

Clear log after sending mail

Syslog Logging

Active

Syslog Server IP Address: (Server NAME or IP Address)

Log Facility: ▾

Active Log and Alert

Log	Send immediate alert:
<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors
<input checked="" type="checkbox"/> System Errors	<input type="checkbox"/> Access Control
<input type="checkbox"/> Access Control	<input type="checkbox"/> Blocked Web Sites
<input type="checkbox"/> TCP Reset	<input type="checkbox"/> Blocked Java etc.
<input type="checkbox"/> Packet Filter	<input type="checkbox"/> Attacks
<input type="checkbox"/> ICMP	<input type="checkbox"/> PKI
<input type="checkbox"/> Remote Management	
<input checked="" type="checkbox"/> CDR	
<input checked="" type="checkbox"/> PPP	
<input type="checkbox"/> Forward Web Sites	
<input type="checkbox"/> Blocked Web Sites	
<input type="checkbox"/> Blocked Java etc.	
<input type="checkbox"/> Attacks	
<input type="checkbox"/> PKI	
<input type="checkbox"/> SSL/TLS	
<input checked="" type="checkbox"/> SIP	

The following table describes the labels in this screen.

Table 64 TOOLS > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server the OX253P should use to e-mail logs and alerts. Leave this field blank if you do not want to send logs or alerts by e-mail.
Mail Subject	Enter the subject line used in e-mail messages the OX253P sends.
Send Log to	Enter the e-mail address to which log entries are sent by e-mail. Leave this field blank if you do not want to send logs by e-mail.
Send Alerts to	Enter the e-mail address to which alerts are sent by e-mail. Leave this field blank if you do not want to send alerts by e-mail.
Log Schedule	<p>Select the frequency with which the OX253P should send log messages by e-mail.</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If the Weekly or the Daily option is selected, specify a time of day when the E-mail should be sent. If the Weekly option is selected, then also specify which day of the week the E-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	<p>This field is only available when you select Weekly in the Log Schedule field.</p> <p>Select which day of the week to send the logs.</p>
Time for Sending Log	<p>This field is only available when you select Daily or Weekly in the Log Schedule field.</p> <p>Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.</p>
Clear log after sending mail	Select this to clear all logs and alert messages after logs are sent by e-mail.
Syslog Logging	
Active	Select this to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that logs the selected categories of logs.
Log Facility	Select a location. The log facility allows you to log the messages in different files in the syslog server. See the documentation of your syslog for more details.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send immediate alert	Select the categories of alerts that you want the OX253P to send immediately.

Table 64 TOOLS > Logs > Log Settings

LABEL	DESCRIPTION
Apply	Click to save your changes.
Cancel	Click to return to the previous screen without saving your changes.

15.4 Log Message Descriptions

The following tables provide descriptions of example log messages.

Table 65 System Error Logs

LOG MESSAGE	DESCRIPTION
WAN connection is down.	The WAN connection is down. You cannot access the network through this interface.
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Table 66 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The device has adjusted its time based on information from the time server.
Time calibration failed	The device failed to get information from the time server.
WAN interface gets IP: %s	The WAN interface got a new IP address from the DHCP or PPPoE server.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the device's web configurator interface.
WEB login failed	Someone has failed to log on to the device's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the device via ftp.
FTP login failed	Someone has failed to log on to the device via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Time initialized by Daytime Server	The device got the time and date from the Daytime server.

Table 66 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Time initialized by Time server	The device got the time and date from the time server.
Time initialized by NTP server	The device got the time and date from the NTP server.
Connect to Daytime server fail	The device was not able to connect to the Daytime server.
Connect to Time server fail	The device was not able to connect to the Time server.
Connect to NTP server fail	The device was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The device dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The device is saving configuration changes.

Table 67 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP UDP IGMP ESP GRE OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP UDP IGMP ESP GRE OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP UDP IGMP ESP GRE OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP UDP IGMP ESP GRE OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.
Firewall allowed a packet that matched a NAT session: [TCP UDP]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

Table 68 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.)
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: <code>sys firewall tcprst</code>).

Table 69 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[TCP UDP ICMP IGMP Generic] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see [Table 76 on page 161](#).

Table 70 ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

Table 71 PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 72 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 73 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule:
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The OX253P cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The OX253P cannot issue a query because TCP/UDP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

For type and code details, see [Table 76 on page 161](#).

Table 74 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [TCP UDP IGMP ESP GRE OSPF]	The firewall detected an IP spoofing attack on the WAN port.

Table 74 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP UDP IGMP ESP GRE OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.

Table 75 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.

Table 75 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

Table 76 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp

Table 76 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

The Status Screen

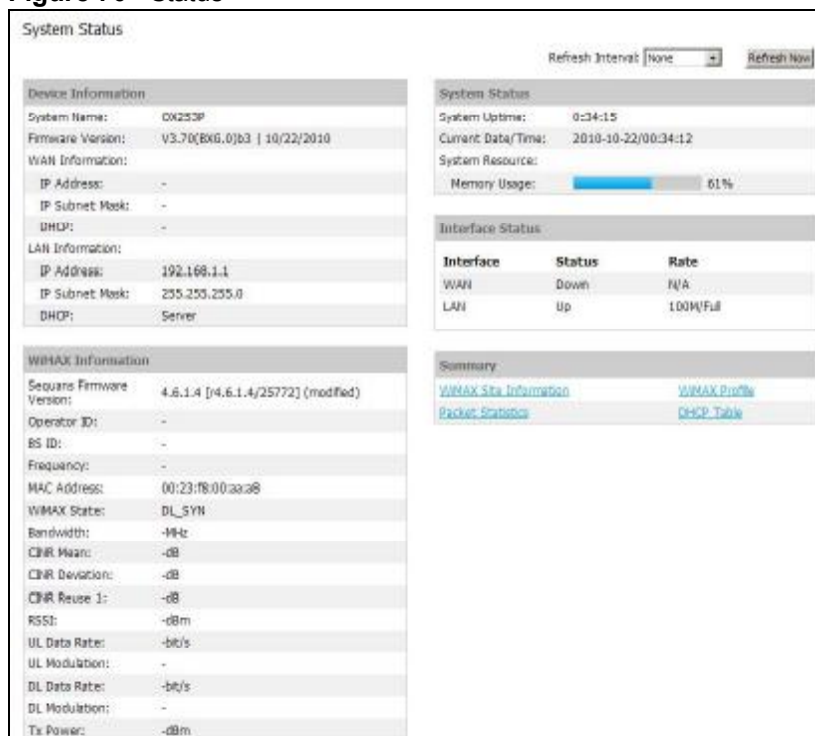
16.1 Overview

Use this screen to view a complete summary of your OX253P connection status.

16.2 Status Screen

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

Figure 70 Status



The following tables describe the labels in this screen.

Table 77 Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the OX253P to update this screen.
Refresh Now	Click this to update this screen immediately.
Device Information	
System Name	This field displays the OX253P system name. It is used for identification. You can change this in the ADVANCED > System Configuration > General screen's System Name field.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in ADVANCED > System Configuration > Firmware .
WAN Information	
IP Address	This field displays the current IP address of the OX253P in the WAN.
IP Subnet Mask	This field displays the current subnet mask on the WAN.
DHCP	This field displays what DHCP services the OX253P is using in the WAN. Choices are: Client - The OX253P is a DHCP client in the WAN. Its IP address comes from a DHCP server on the WAN. None - The OX253P is not using any DHCP services in the WAN. It has a static IP address.
LAN Information	
IP Address	This field displays the current IP address of the OX253P in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the OX253P is providing to the LAN. Choices are: Server - The OX253P is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The OX253P is routing DHCP requests to one or more DHCP servers. The DHCP server(s) may be on another network. None - The OX253P is not providing any DHCP services to the LAN. You can change this in ADVANCED > LAN Configuration > DHCP Setup .
WiMAX Information	
Sequans Firmware Version	This field displays the firmware version of the WiMAX chipset on the OX253P.
Operator ID	Every WiMAX service provider has a unique Operator ID number, which is broadcast by each base station it owns. You can only connect to the Internet through base stations belonging to your service provider's network.
BS ID	This field displays the identification number of the wireless base station to which the OX253P is connected. Every base station transmits a unique BSID, which identifies it across the network.

Table 77 Status (continued)

LABEL	DESCRIPTION
Frequency	This field displays the radio frequency of the OX253P's wireless connection to a base station.
MAC address	This field displays the Media Access Control address of the OX253P. Every network device has a unique MAC address which identifies it across the network.
WiMAX State	<p>This field displays the status of the OX253P's current connection.</p> <ul style="list-style-type: none"> • INIT: the OX253P is starting up. • DL_SYN: The OX253P is unable to connect to a base station. • RANGING: the OX253P and the base station are transmitting and receiving information about the distance between them. Ranging allows the OX253P to use a lower transmission power level when communicating with a nearby base station, and a higher transmission power level when communicating with a distant base station. • CAP_NEGO: the OX253P and the base station are exchanging information about their capabilities. • AUTH: the OX253P and the base station are exchanging security information. • REGIST: the OX253P is registering with a RADIUS server. • OPERATIONAL: the OX253P has successfully registered with the base station. Traffic can now flow between the OX253P and the base station. • IDLE: the OX253P is in power saving mode, but can connect when a base station alerts it that there is traffic waiting.
Bandwidth	This field shows the size of the bandwidth step the OX253P uses to connect to a base station in megahertz (MHz).
CINR Mean	This field shows the average Carrier to Interference plus Noise Ratio of the current connection. This value is an indication of overall radio signal quality. A higher value indicates a higher signal quality, and a lower value indicates a lower signal quality.
CINR Deviation	This field shows the amount of change in the CINR level. This value is an indication of radio signal stability. A lower number indicates a more stable signal, and a higher number indicates a less stable signal.
CINR Reuse 1	This field shows the WiMAX signal quality when the OX253P is transmitting data to the base station. A higher value indicates a higher signal quality, and a lower value indicates a lower signal quality. The base station determines downlink (DL) and uplink (UL) modulations based on this value.
RSSI	<p>This field shows the Received Signal Strength Indication. This value is a measurement of overall radio signal strength. A higher RSSI level indicates a stronger signal, and a lower RSSI level indicates a weaker signal.</p> <p>A strong signal does not necessarily indicate a good signal: a strong signal may have a low signal-to-noise ratio (SNR).</p>
UL Data Rate	This field shows the number of data packets uploaded from the OX253P to the base station each second.

Table 77 Status (continued)

LABEL	DESCRIPTION
UL Modulation	<p>This field shows the modulation technique (QPSK or 16-QAM) the OX253P is using for transmitting data to the base station. 16-QAM modulation gets higher transmission rate because it carries more data than QPSK. The possible values of this field are qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4.</p> <p>See Section 16.3 on page 171 for more information.</p>
DL Data Rate	<p>This field shows the number of data packets downloaded to the OX253P from the base station each second.</p>
DL Modulation	<p>This field shows the modulation technique (QPSK, 16-QAM or 64-QAM) the base station is using for transmitting data to the OX253P. 64-QAM modulation gets higher transmission rate because it carries more data than QPSK and 16-QAM. The possible values of this field are qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-1/2, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6.</p> <p>See Section 16.3 on page 171 for more information.</p>
Tx Power	<p>This field shows the output transmission (Tx) level of the OX253P.</p>
System Status	
System Uptime	<p>This field displays how long the OX253P has been running since it last started up. The OX253P starts up when you plug it in, when you restart it (ADVANCED > System Configuration > Restart), or when you reset it.</p>
Current Date/Time	<p>This field displays the current date and time in the OX253P. You can change this in SETUP > Time Setting.</p>
Memory Usage	<p>This field displays what percentage of the OX253P's memory is currently used. The higher the memory usage, the more likely the OX253P is to slow down. Some memory is required just to start the OX253P and to run the web configurator. You can reduce the memory usage by disabling some services (see CPU Usage); 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.</p>
Interface Status	
Interface	<p>This column displays each interface of the OX253P.</p>
Status	<p>This field indicates whether or not the OX253P is using the interface.</p> <p>For the WAN interface, this field displays Up when the OX253P is connected to a WiMAX network, and Down when the OX253P is not connected to a WiMAX network.</p> <p>For the LAN interface, this field displays Up when the OX253P is using the interface and Down when the OX253P is not using the interface.</p>
Rate	<p>For the LAN ports this displays the port speed and duplex setting.</p> <p>For the WAN interface, it displays the downstream and upstream transmission rate or N/A if the OX253P is not connected to a base station.</p> <p>For the WLAN interface, it displays the transmission rate when WLAN is enabled or N/A when WLAN is disabled.</p>

Table 77 Status (continued)

LABEL	DESCRIPTION
Summary	
WiMAX Site Information	Click this link to view details of the radio frequencies used by the OX253P to connect to a base station.
WiMAX Profile	Click this link to view details of the current wireless security settings.
Packet Statistics	Click this link to view port status and packet specific statistics.
DHCP Table	Click this link to see details of computers to which the OX253P has given an IP address.

16.2.1 Packet Statistics

Click **Status > Packet Statistics** to open this screen. This read-only screen displays information about the data transmission through the OX253P. To configure these settings, go to the corresponding area in the **Advanced** screens.

Figure 71 Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	11091	9262	0	64	593	5:58:17

System Up Time: 6:00:02

Poll Interval : 500 sec

The following table describes the fields in this screen.

Table 78 Packet Statistics

LABEL	DESCRIPTION
Port	This column displays each interface of the OX253P.
Status	This field indicates whether or not the OX253P is using the interface. For the WAN interface, this field displays the port speed and duplex setting when the OX253P is connected to a WiMAX network, and Down when the OX253P is not connected to a WiMAX network. For the LAN interface, this field displays the port speed and duplex setting when the OX253P is using the interface and Down when the OX253P is not using the interface. For the WLAN interface, it displays the transmission rate when WLAN is enabled or Down when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this interface.

Table 78 Packet Statistics (continued)

LABEL	DESCRIPTION
RxPkts	This field displays the number of packets received on this interface.
Collisions	This field displays the number of collisions on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this interface has been connected.
System up Time	This is the elapsed time the system has been on.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval field above.
Stop	Click this button to halt the refreshing of the system statistics.

16.2.2 WiMAX Site Information

Click **Status > WiMAX Site Information** to open this screen. This read-only screen shows WiMAX frequency information for the OX253P. These settings can be configured in the **ADVANCED > WAN Configuration > WiMAX Configuration** screen.

Figure 72 WiMAX Configuration

DL Frequency [1]:	<input type="text" value="2665500"/>	kHz
DL Frequency [2]:	<input type="text" value="2675500"/>	kHz
DL Frequency [3]:	<input type="text" value="2685500"/>	kHz
DL Frequency [4]:	<input type="text" value="0"/>	kHz
DL Frequency [5]:	<input type="text" value="0"/>	kHz
DL Frequency [6]:	<input type="text" value="0"/>	kHz
DL Frequency [7]:	<input type="text" value="0"/>	kHz
DL Frequency [8]:	<input type="text" value="0"/>	kHz
DL Frequency [9]:	<input type="text" value="0"/>	kHz
DL Frequency [10]:	<input type="text" value="0"/>	kHz
DL Frequency [11]:	<input type="text" value="0"/>	kHz
DL Frequency [12]:	<input type="text" value="0"/>	kHz
DL Frequency [13]:	<input type="text" value="0"/>	kHz
DL Frequency [14]:	<input type="text" value="0"/>	kHz
DL Frequency [15]:	<input type="text" value="0"/>	kHz
DL Frequency [16]:	<input type="text" value="0"/>	kHz
DL Frequency [17]:	<input type="text" value="0"/>	kHz
DL Frequency [18]:	<input type="text" value="0"/>	kHz
DL Frequency [19]:	<input type="text" value="0"/>	kHz
Bandwidth :	<input type="text" value="10000"/>	KHz

The following table describes the labels in this screen.

Table 79 WiMAX Configuration

LABEL	DESCRIPTION
DL Frequency [1] ~ [19]	These fields show the downlink frequency settings in kilohertz (kHz). These settings determine how the OX253P searches for an available wireless connection.

16.2.3 DHCP Table

Click **Status > DHCP Table** to open this screen. This read-only screen shows the IP addresses, Host Names and MAC addresses of the devices currently connected to the OX253P. These settings can be configured in the **ADVANCED > LAN Configuration > DHCP Setup** screen.

Figure 73 DHCP Table

The screenshot shows a web interface titled "DHCP Table". It contains a table with the following data:

#	IP Address	Host Name	MAC Address
1	192.168.100.33	TWPC13435-XP	00:02:e3:56:16:9d

Below the table is a "Refresh" button.

Each field is described in the following table.

Table 80 DHCP Table

LABEL	DESCRIPTION
#	The number of the item in this list.
IP Address	This field displays the IP address the OX253P assigned to a computer in the network.
Host Name	This field displays the system name of the computer to which the OX253P assigned the IP address.
MAC Address	This field displays the MAC address of the computer to which the OX253P assigned the IP address.
Refresh	Click this button to update the table data.

16.2.4 WiMAX Profile

Click **Status > WiMAX Profile** to open this screen. This read-only screen displays information about the security settings you are using. To configure these settings, go to the **ADVANCED > WAN Configuration > Internet Connection** screen.

Note: Not all OX253P models have all the fields shown here.

Figure 74 WiMAX Profile

The screenshot shows a configuration window titled 'WiMAX Profile'. It contains the following fields and their values:

- User Name: [Empty text box]
- Password: [Empty text box]
- Anonymous Identity: [Empty text box]
- PKM: [Dropdown menu showing PKMV2]
- Authentication: [Dropdown menu showing TTLS]
- TTLS Inner EAP: [Dropdown menu showing PAP]
- Certificate: [Empty text box]

The following table describes the labels in this screen.

Table 81 The WiMAX Profile Screen

LABEL	DESCRIPTION
User Name	This is the username for your Internet access account.
Password	This is the password for your Internet access account. The password displays as a row of asterisks for security purposes.
Anonymous Identity	This is the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption.
PKM	This field displays the Privacy Key Management version number. PKM provides security between the OX253P and the base station. See the WiMAX security appendix for more information.
Authentication	This field displays the user authentication method. Authentication is the process of confirming the identity of a user (by means of a username and password, for example). EAP-TTLS allows an MS/SS and a base station to establish a secure link (or 'tunnel') with an AAA (Authentication, Authorization and Accounting) server in order to exchange authentication information. See the WiMAX security appendix for more details.

Table 81 The WiMAX Profile Screen (continued)

LABEL	DESCRIPTION
TTLS Inner EAP	<p>This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details.</p> <p>The OX253P supports the following inner authentication types:</p> <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol)
Certificate	This is the security certificate the OX253P uses to authenticate the AAA server, if one is available.

16.3 Technical Reference

The following section contains additional technical information about the OX253P features described in this chapter.

Modulation

A modulation technique is a method used to encode digital or analog information onto an analog carrier signal so it can be transmitted. A device modulates digital data onto an radio signal to send over the wireless network. The receiving device demodulates the radio signals back to digital data. The specific frequency at which the information is modulated on the radio signal is called the carrier.

QPSK

The Quadrature Phase-Shift Keying digital modulation technique is used in WiMAX networks to transmit downlink traffic using a maximum data rate of 9.5 Mbps.

16QAM

The Quadrature Amplitude Modulation (QAM) digital modulation technique modulates (changes) the amplitude of two carrier waves. WiMAX networks use 16QAM to transmit downlink traffic using a data rate of 18 Mbps.

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](#)
- [OX253P Access and Login](#)
- [Internet Access](#)
- [Export a Certificate File](#)

17.1 Power, Hardware Connections, and LEDs

The OX253P does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adapter or cord included with the OX253P.
- 2 Make sure the power adapter or cord is connected to the OX253P 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 OX253P.
- 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 20](#) 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 OX253P.
- 5 If the problem continues, contact the vendor.

I hear beeping sounds coming from the OX253P.

- 1 When the OX253P receives signals from a base station, it beeps to notify you.
- 2 If you do not want to hear beeps from the OX253P, log into the Web Configurator and disable the buzzer in the **ADVANCED > WAN Configuration > Buzzer** screen.

17.2 OX253P Access and Login

I forgot the IP address for the OX253P.

- 1 The default IP address is <http://192.168.1.1>.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the OX253P 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 OX253P (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 OX253P to its factory defaults. See [Section 17.1 on page 173](#).

I forgot the password.

- 1 The default password of the administrator account is **admin**.
- 2 If this does not work, you have to reset the OX253P to its factory defaults. See [Section 9.5 on page 93](#).

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 <http://192.168.1.1>.
 - If you changed the IP address ([Section 5.2 on page 48](#)), 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 OX253P](#).
- 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 20](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Appendix C on page 217](#).
- 4 If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. Your OX253P 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 OX253P. See [Appendix D on page 229](#).
- 5 Reset the OX253P to its factory defaults, and try to access the OX253P with the default IP address. See [Section 9.6 on page 95](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the OX253P using another service, such as Telnet. If you can access the OX253P, check the remote management settings and firewall rules to find out why the OX253P 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 OX253P.

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **admin**. 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 OX253P. Log out of the OX253P 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 OX253P.
- 4 If this does not work, you have to reset the OX253P to its factory defaults. See [Section 9.5 on page 93](#).

I cannot Telnet to the OX253P.

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

17.3 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 20](#).
- 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. In the web configurator, go to the **Status** screen. Click the **WiMAX Profile** link in the **Summary** box and make sure that you are using the correct security settings for your Internet account.
- 4 Check your WiMAX settings. The OX253P may have been set to search the wrong frequencies for a wireless connection. In the web configurator, go to the **Status** screen. Click the **WiMAX Site Information** link in the **Summary** box and ensure that the values are correct. If the values are incorrect, enter the correct frequency settings in the **ADVANCED > WAN Configuration > WiMAX Configuration** screen. 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 OX253P, 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 OX253P), 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 20](#).
- 2 Disconnect and re-connect the power adapter to the OX253P.
- 3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- 1 The quality of the OX253P's wireless connection to the base station may be poor. Poor signal reception may be improved by moving the OX253P 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 OX253P 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 20](#). If the OX253P 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 OX253P.
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

The Internet connection disconnects.

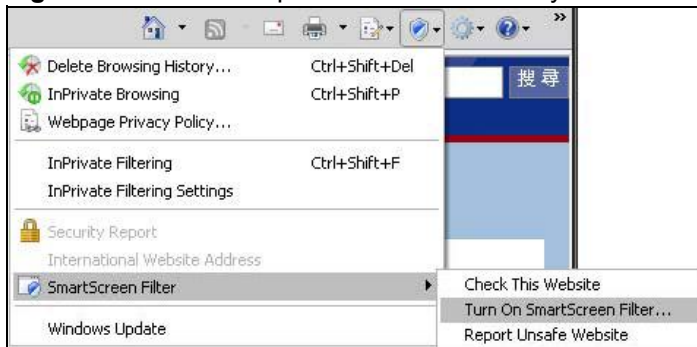
- 1 Check your WiMAX link and signal strength using the **WiMAX Link and Strength Indicator** LEDs on the device.
- 2 Contact your ISP if the problem persists.

17.4 Export a Certificate File

When I try to export a certificate file from the OX253P, the exporting process hangs.

- 1 You may encounter this issue if you are using Internet Explorer 8.
- 2 Make sure you have upgraded to Internet Explorer 8 standard version.
- 3 To resolve this, select **Tool > SmartScreen Filter > Turn On SmartScreen Filter** in your browser.

Figure 75 Internet Explorer 8: Turn On Safety Filter



- 4 Select **Turn off SmartScreen Filter** and click **OK**. Export the certificate file again, you should be able to download the file now.

Figure 76 Internet Explorer 8: Turn Off Safety Filter



17.5 Reset the OX253P to Its Factory Defaults

If you reset the OX253P, you lose all of the changes you have made. The OX253P re-loads its default settings, and the password resets to **admin**. You have to make all of your changes again.

17.5.1 Pop-up Windows, JavaScripts and Java Permissions

Please see [Appendix C on page 217](#).

Product Specifications

This chapter gives details about your OX253P's hardware and firmware features.

Table 82 Environmental and Hardware Specifications

FEATURE	DESCRIPTION
Operating Temperature	-15°C to 60°C (ODU), -10°C to 55°C (IDU)
Storage Temperature	-15°C to 65°C (ODU), -15°C to 60°C (IDU)
Operating Humidity	10% ~ 90% (non-condensing)
Storage Humidity	10% to 95% (non-condensing)
Power Supply	Input: AC Voltage Range: 90 VAC - 270 VAC AC Voltage Rating: 100 VAC - 240 VAC Output: 48VDC, 0.38A Max.
Power Consumption	US: maximum 18.24W, average 7.932W EU: maximum 12.12W
Ethernet Interface	One auto-negotiating, auto-MDI/MDI-X NWay 10/100 Mbps RJ-45 Ethernet port
Power over Ethernet Interface (PoE)	One RJ-45-type PoE port providing 48V DC to the OX253P-ODU from the OX253P-IDU
Antennas	One 15dBi \pm 0.5dBi Cross-Polarization antenna (ODU)
Weight	400g
Dimensions	ODU: 372 (L) mm x 232 (W) mm x 54.8 (H) mm IDU: 188.5 (L) mm x 131.2 (W) mm x 42 (H) mm

Table 83 Radio Specifications

FEATURE	DESCRIPTION
WiMAX Operating Frequency	2.5~2.7 GHz
Channel Bandwidth	5MHz / 10MHz
Maximum Transmit Power	26dbm with ODU antenna deployed.
WiMAX Compliance	Compliant to receiver performances defined in IEEE P802.16-2005, §8.4.13.

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 OX253P. You must connect using a compatible web browser in order to use it.
High Speed Wireless Internet Access	The OX253P 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 OX253P is a WiMAX mobile station (MS) compatible with the IEEE 802.16e standard.
Firewall	The OX253P 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 OX253P's firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	The OX253P 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.
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.

Table 84 Firmware Specifications (continued)

FEATURE	DESCRIPTION
Time and Date	Get the current time and date from an external server when you turn on your OX253P. You can also set the time manually.
Logging	Use the OX253P's logging feature to view connection history, surveillance logs, and error messages.

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 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 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 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 3261	Session Initiation Protocol (SIP version 2)
RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP).
RFC 3550	RTP - A Real Time Protocol for Real-Time Applications
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)-XR
RFC 3715	IP Sec/NAT Compatibility
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

A

WiMAX Security

Wireless security is vital to protect your wireless communications. Without it, information transmitted over the wireless network would be accessible to any networking device within range.

User Authentication and Data Encryption

The WiMAX (IEEE 802.16) standard employs user authentication and encryption to ensure secured communication at all times.

User authentication is the process of confirming a user's identity and level of authorization. Data encryption is the process of encoding information so that it cannot be read by anyone who does not know the code.

WiMAX uses PKMv2 (Privacy Key Management version 2) for authentication, and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol) for data encryption.

WiMAX supports EAP (Extensible Authentication Protocol, RFC 2486) which allows additional authentication methods to be deployed with no changes to the base station or the mobile or subscriber stations.

PKMv2

PKMv2 is a procedure that allows authentication of a mobile or subscriber station and negotiation of a public key to encrypt traffic between the MS/SS and the base station. PKMv2 uses standard EAP methods such as Transport Layer Security (EAP-TLS) or Tunneled TLS (EAP-TTLS) for secure communication.

In cryptography, a 'key' is a piece of information, typically a string of random numbers and letters, that can be used to 'lock' (encrypt) or 'unlock' (decrypt) a message. Public key encryption uses key pairs, which consist of a public (freely available) key and a private (secret) key. The public key is used for encryption and the private key is used for decryption. You can decrypt a message only if you have the private key. Public key certificates (or 'digital IDs') allow users to verify each other's identity.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The base station is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- **Authentication**
Determines the identity of the users.
- **Authorization**
Determines the network services available to authenticated users once they are connected to the network.
- **Accounting**
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your base station acts as a message relay between the MS/SS and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the base station and the RADIUS server for user authentication:

- **Access-Request**
Sent by an base station requesting authentication.
- **Access-Reject**
Sent by a RADIUS server rejecting access.
- **Access-Accept**
Sent by a RADIUS server allowing access.
- **Access-Challenge**
Sent by a RADIUS server requesting more information in order to allow access. The base station sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the base station and the RADIUS server for user accounting:

- **Accounting-Request**
Sent by the base station requesting accounting.
- **Accounting-Response**
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password they both know. The key is not sent over

the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Diameter

Diameter (RFC 3588) is a type of AAA server that provides several improvements over RADIUS in efficiency, security, and support for roaming.

Security Association

The set of information about user authentication and data encryption between two computers is known as a security association (SA). In a WiMAX network, the process of security association has three stages.

- Authorization request and reply

The MS/SS presents its public certificate to the base station. The base station verifies the certificate and sends an authentication key (AK) to the MS/SS.

- Key request and reply

The MS/SS requests a transport encryption key (TEK) which the base station generates and encrypts using the authentication key.

- Encrypted traffic

The MS/SS decrypts the TEK (using the authentication key). Both stations can now securely encrypt and decrypt the data flow.

CCMP

All traffic in a WiMAX network is encrypted using CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol). CCMP is based on the 128-bit Advanced Encryption Standard (AES) algorithm.

'Counter mode' refers to the encryption of each block of plain text with an arbitrary number, known as the counter. This number changes each time a block of plain text is encrypted. Counter mode avoids the security weakness of repeated identical blocks of encrypted text that makes encrypted data vulnerable to pattern-spotting.

'Cipher Block Chaining Message Authentication' (also known as CBC-MAC) ensures message integrity by encrypting each block of plain text in such a way that its encryption is dependent on the block before it. This series of 'chained' blocks creates a message authentication code (MAC or CMAC) that ensures the encrypted data has not been tampered with.

Authentication

The OX253P supports EAP-TTLS authentication.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection (with EAP-TLS digital certifications are needed by both the server and the wireless clients for mutual authentication). 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.

B

Setting Up Your Computer's IP Address

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

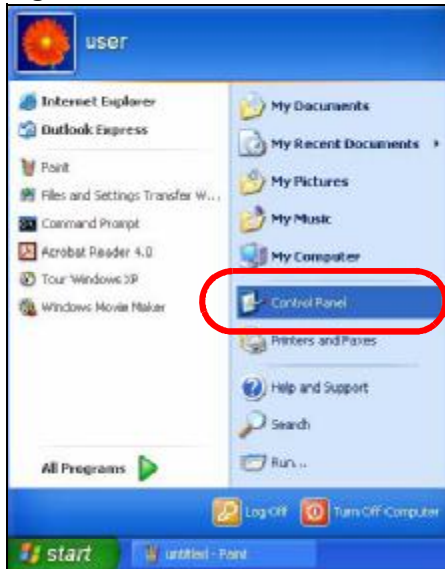
- [Windows XP/NT/2000 on page 190](#)
- [Windows Vista on page 193](#)
- [Mac OS X: 10.3 and 10.4 on page 197](#)
- [Mac OS X: 10.5 on page 201](#)
- [Linux: Ubuntu 8 \(GNOME\) on page 204](#)
- [Linux: openSUSE 10.3 \(KDE\) on page 210](#)

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

- 1 Click **Start > Control Panel**.

Figure 77 Windows XP: Start Menu



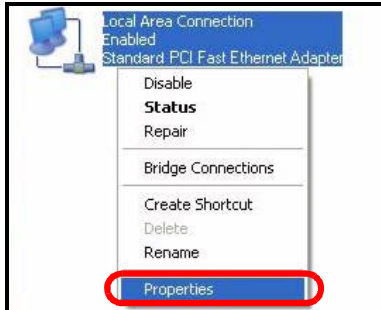
- 2 In the **Control Panel**, click the **Network Connections** icon.

Figure 78 Windows XP: Control Panel



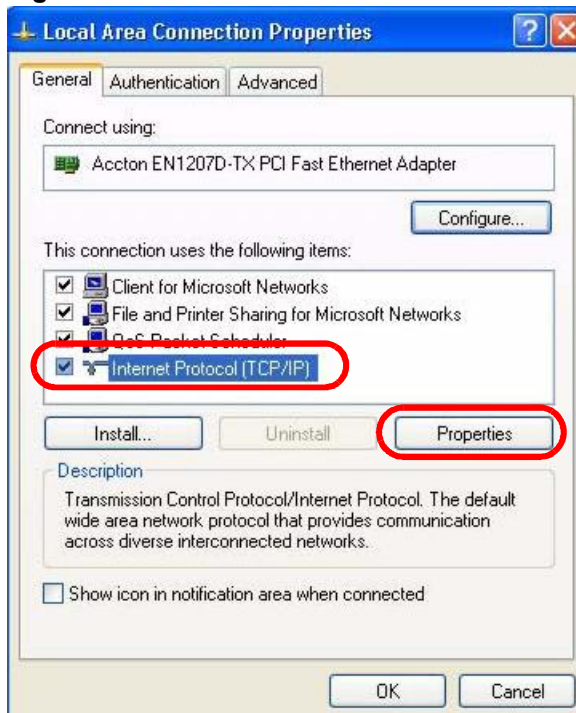
- 3 Right-click **Local Area Connection** and then select **Properties**.

Figure 79 Windows XP: Control Panel > Network Connections > Properties



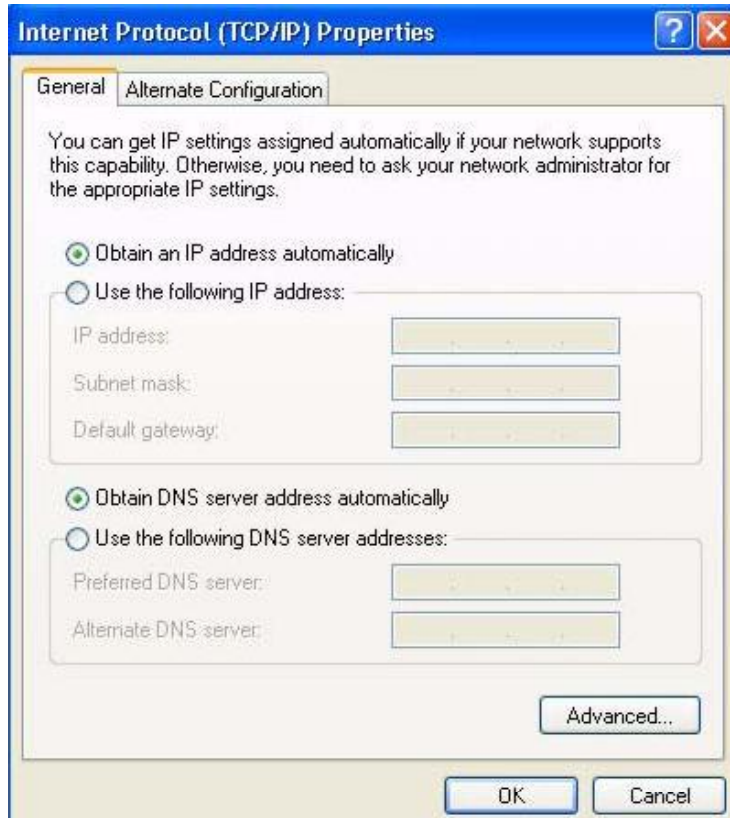
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 80 Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 81 Windows XP: Internet Protocol (TCP/IP) Properties



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

Click **OK** to close the **Local Area Connection Properties** window. **Verifying Settings**

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

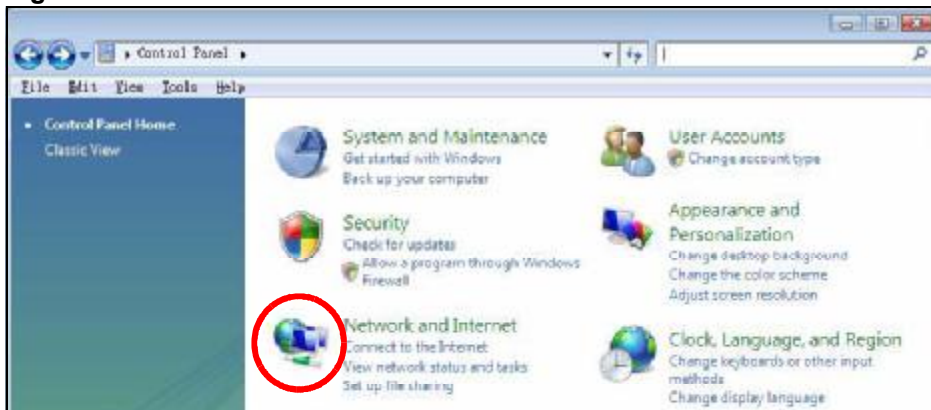
- 1 Click **Start > Control Panel**.

Figure 82 Windows Vista: Start Menu



- 2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 83 Windows Vista: Control Panel



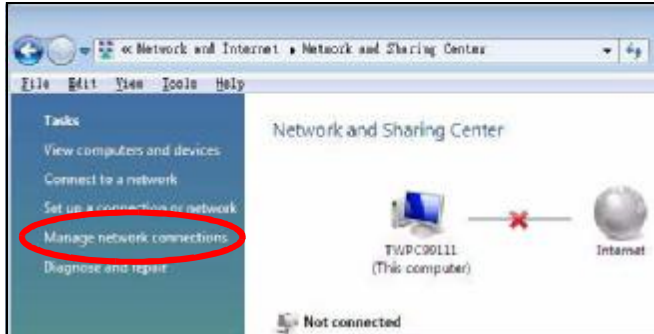
- 3 Click the **Network and Sharing Center** icon.

Figure 84 Windows Vista: Network And Internet



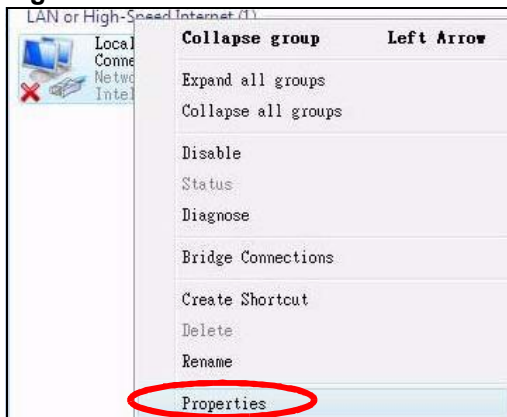
- 4 Click **Manage network connections**.

Figure 85 Windows Vista: Network and Sharing Center



- 5 Right-click **Local Area Connection** and then select **Properties**.

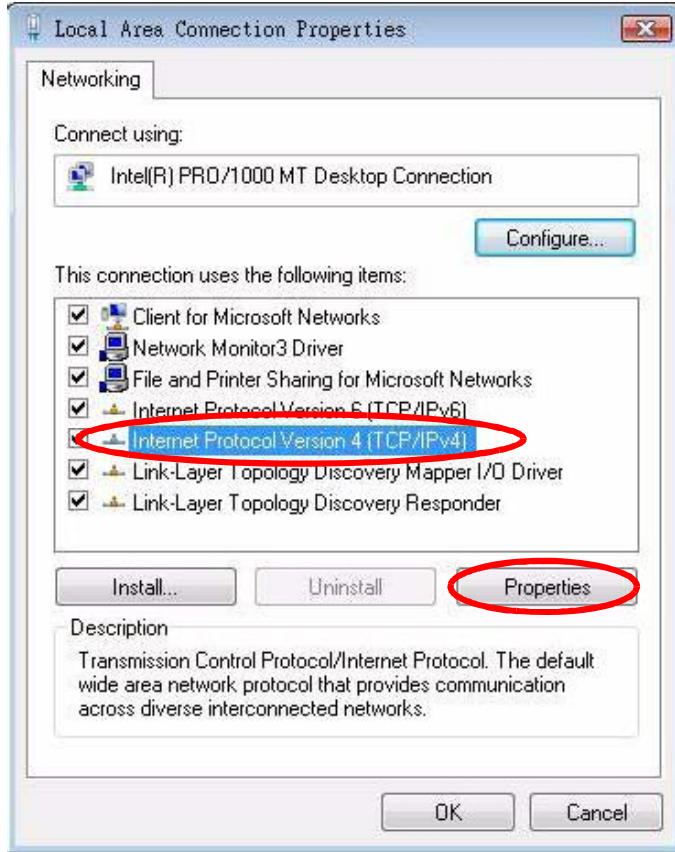
Figure 86 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 87 Windows Vista: Local Area Connection Properties



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 88 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



- 8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced**.

- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

Click **OK** to close the **Local Area Connection Properties** window. **Verifying Settings**

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

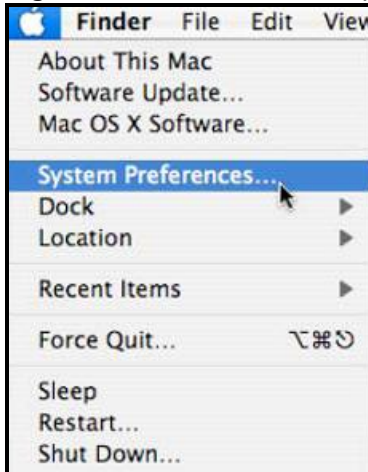
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

- 1 Click **Apple > System Preferences**.

Figure 89 Mac OS X 10.4: Apple Menu



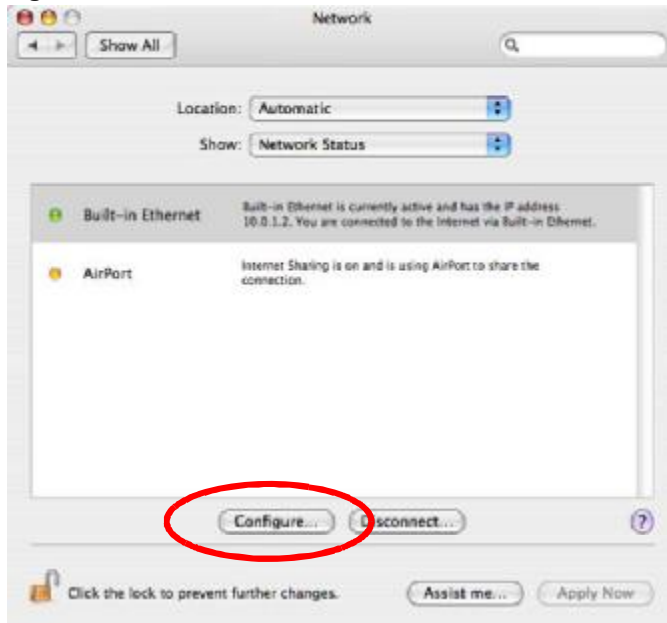
- 2 In the **System Preferences** window, click the **Network** icon.

Figure 90 Mac OS X 10.4: System Preferences



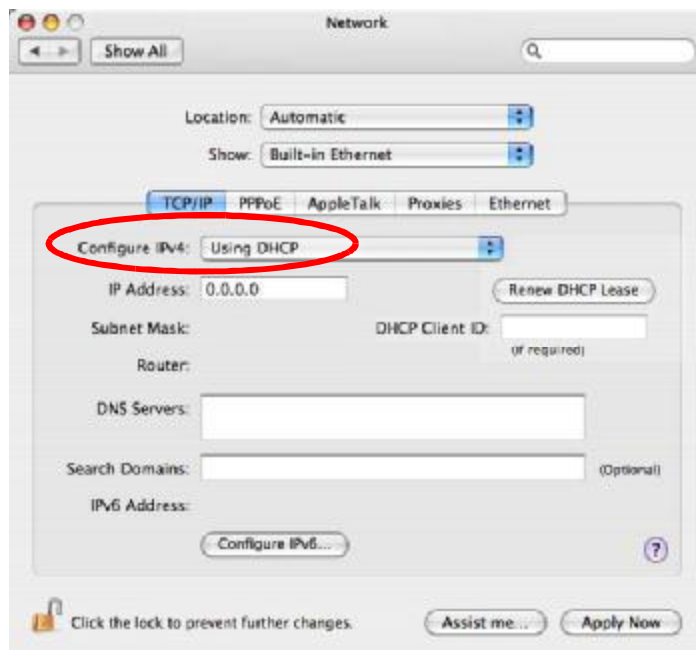
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

Figure 91 Mac OS X 10.4: Network Preferences



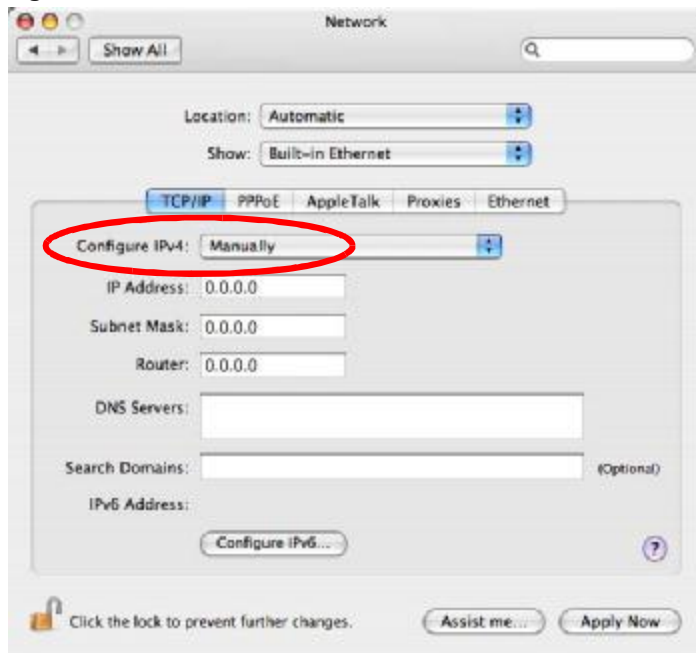
- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 92 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



- 5 For statically assigned settings, do the following:
 - From the **Configure IPv4** list, select **Manually**.
 - In the **IP Address** field, type your IP address.
 - In the **Subnet Mask** field, type your subnet mask.
 - In the **Router** field, type the IP address of your device.

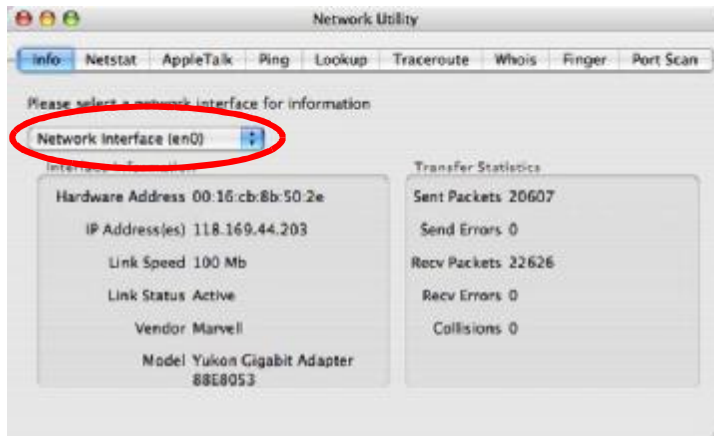
Figure 93 Mac OS X 10.4: Network Preferences > Ethernet



Click **Apply Now** and close the window. **Verifying Settings**

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 94 Mac OS X 10.4: Network Utility

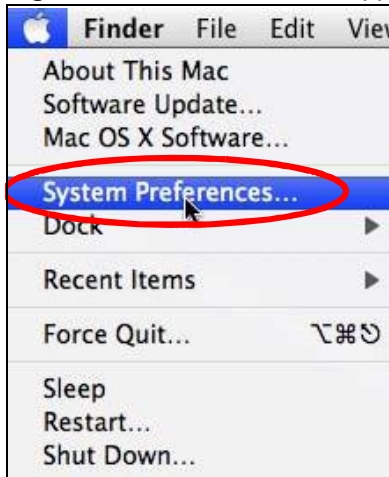


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

- 1 Click **Apple > System Preferences**.

Figure 95 Mac OS X 10.5: Apple Menu



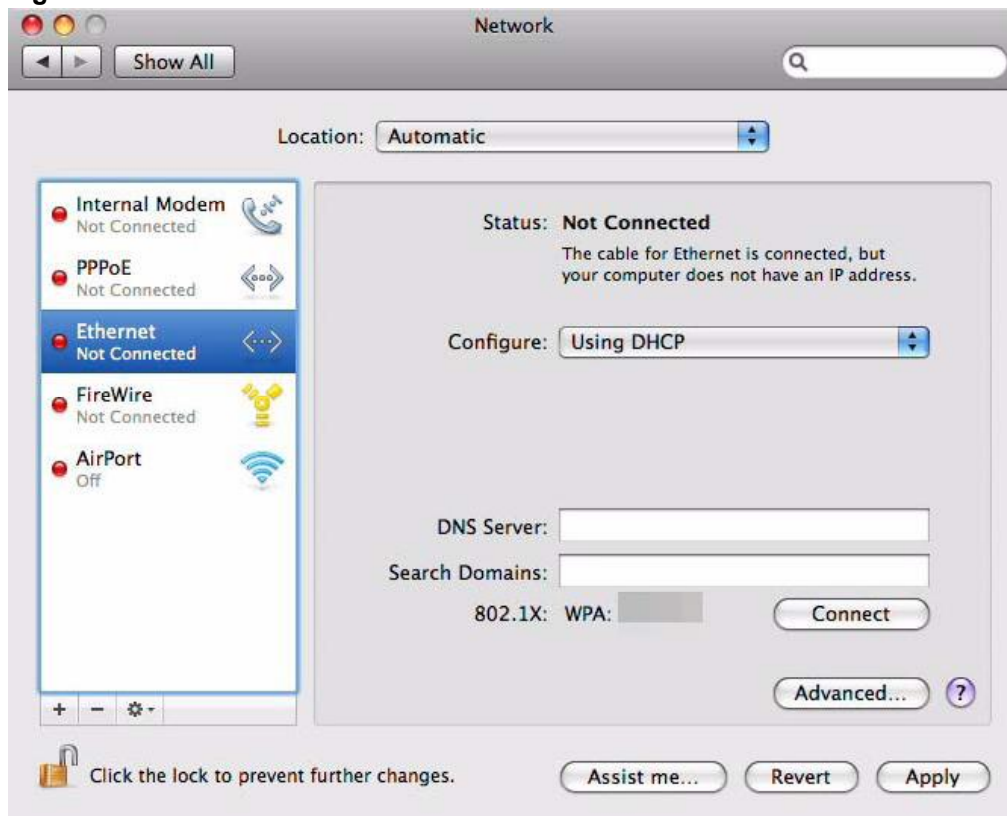
- 2 In System Preferences, click the **Network** icon.

Figure 96 Mac OS X 10.5: Systems Preferences



- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

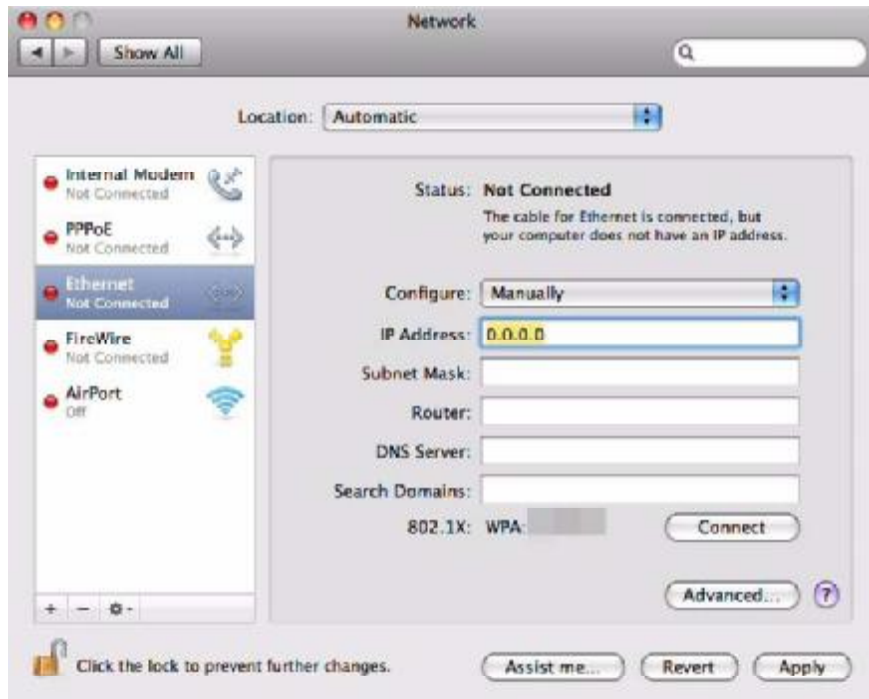
Figure 97 Mac OS X 10.5: Network Preferences > Ethernet



- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.
- 5 For statically assigned settings, do the following:
 - From the **Configure** list, select **Manually**.
 - In the **IP Address** field, enter your IP address.
 - In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your OX253P.

Figure 98 Mac OS X 10.5: Network Preferences > Ethernet

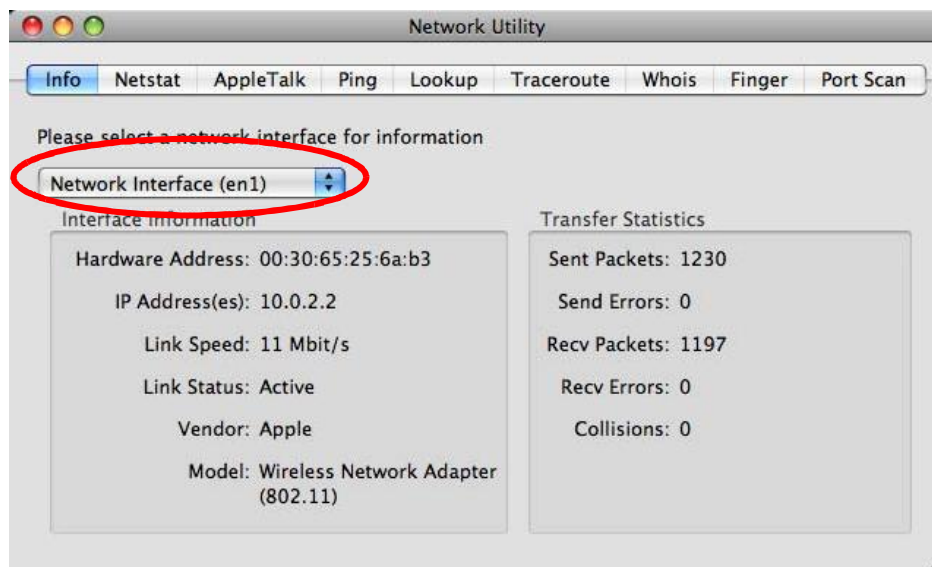


- 6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network** interface from the **Info** tab.

Figure 99 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

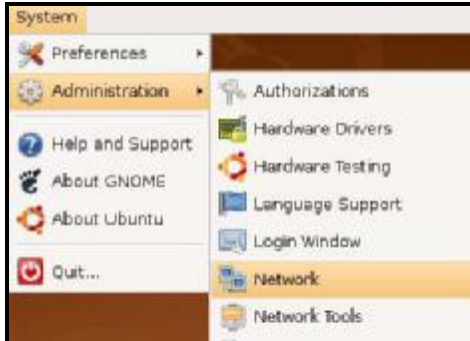
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

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

Follow the steps below to configure your computer IP address in GNOME:

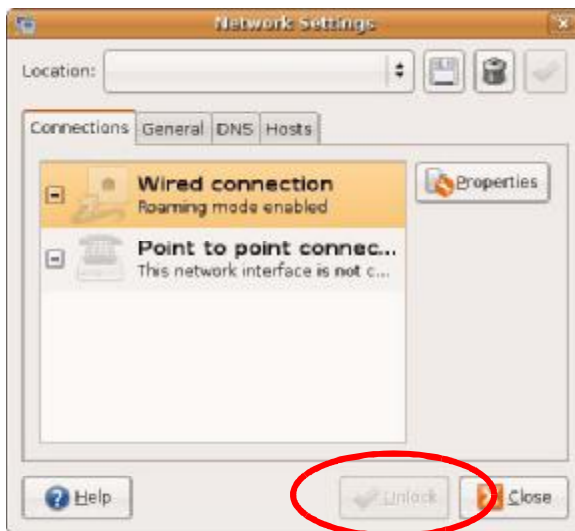
- 1 Click **System > Administration > Network**.

Figure 100 Ubuntu 8: System > Administration Menu



- 2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 101 Ubuntu 8: Network Settings > Connections



- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 102 Ubuntu 8: Administrator Account Authentication



- 4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 103 Ubuntu 8: Network Settings > Connections



- 5 The **Properties** dialog box opens.

Figure 104 Ubuntu 8: Network Settings > Properties



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
 - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

- 7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 105 Ubuntu 8: Network Settings > DNS



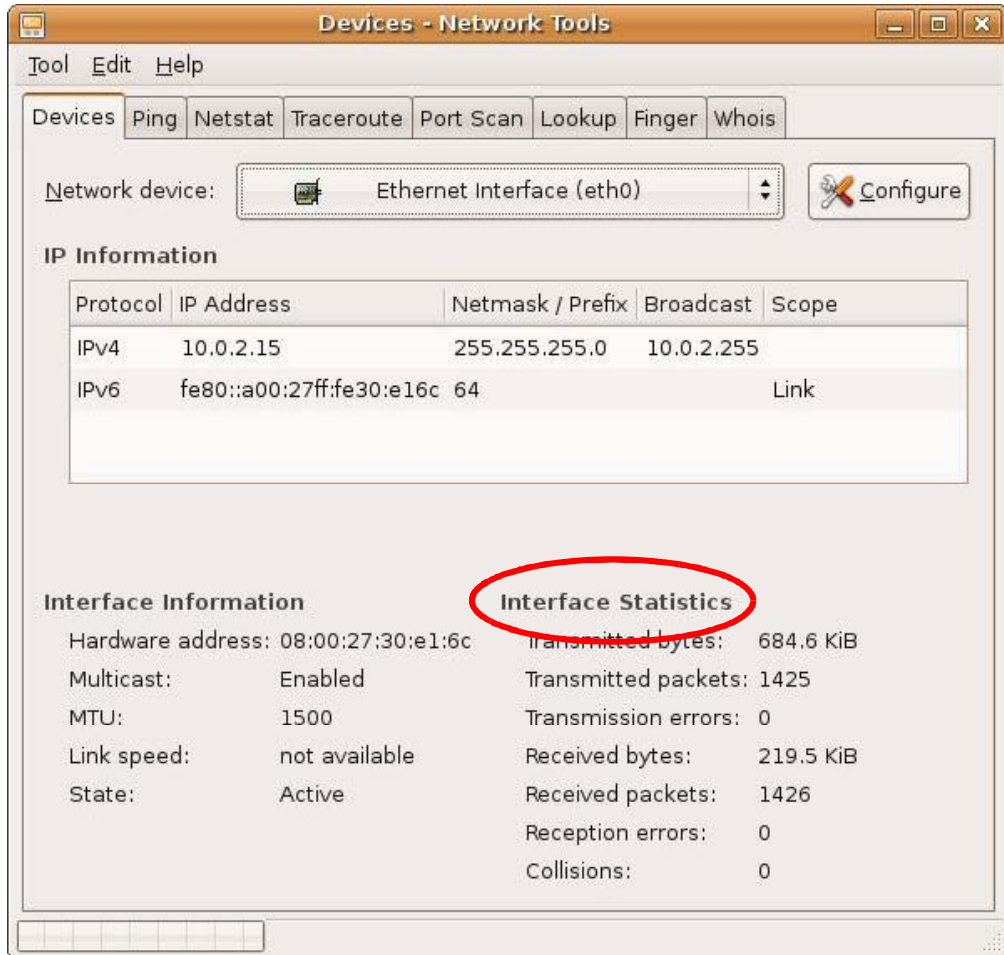
- 8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network** device from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 106 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

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

Follow the steps below to configure your computer IP address in the KDE:

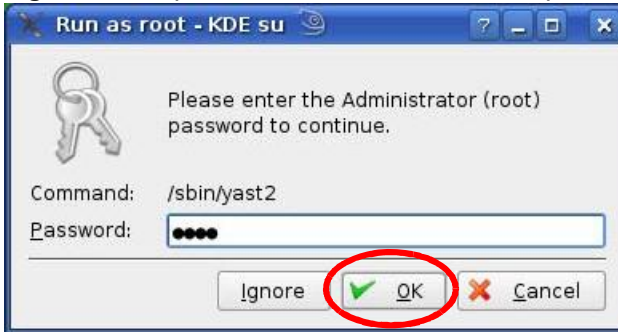
- 1 Click K Menu > Computer > Administrator Settings (YaST).

Figure 107 openSUSE 10.3: K Menu > Computer Menu



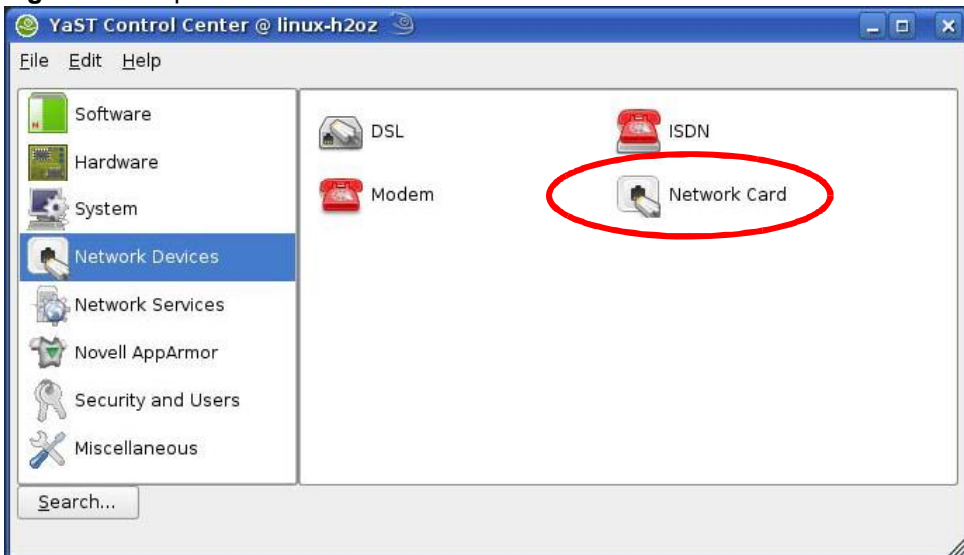
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 108 openSUSE 10.3: K Menu > Computer Menu



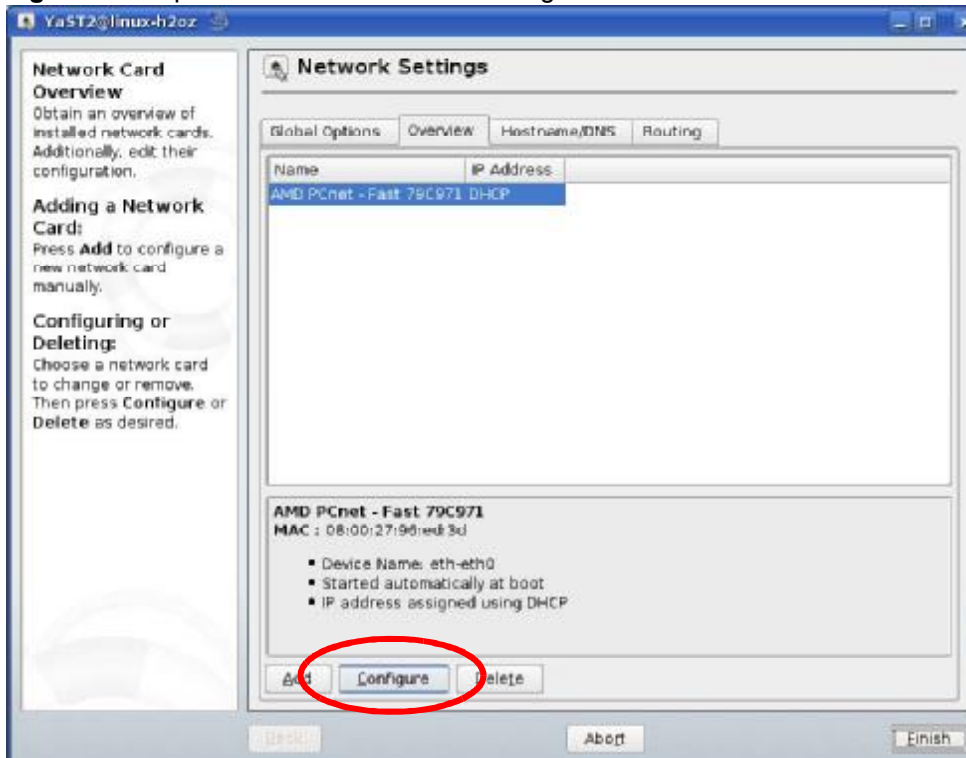
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 109 openSUSE 10.3: YaST Control Center



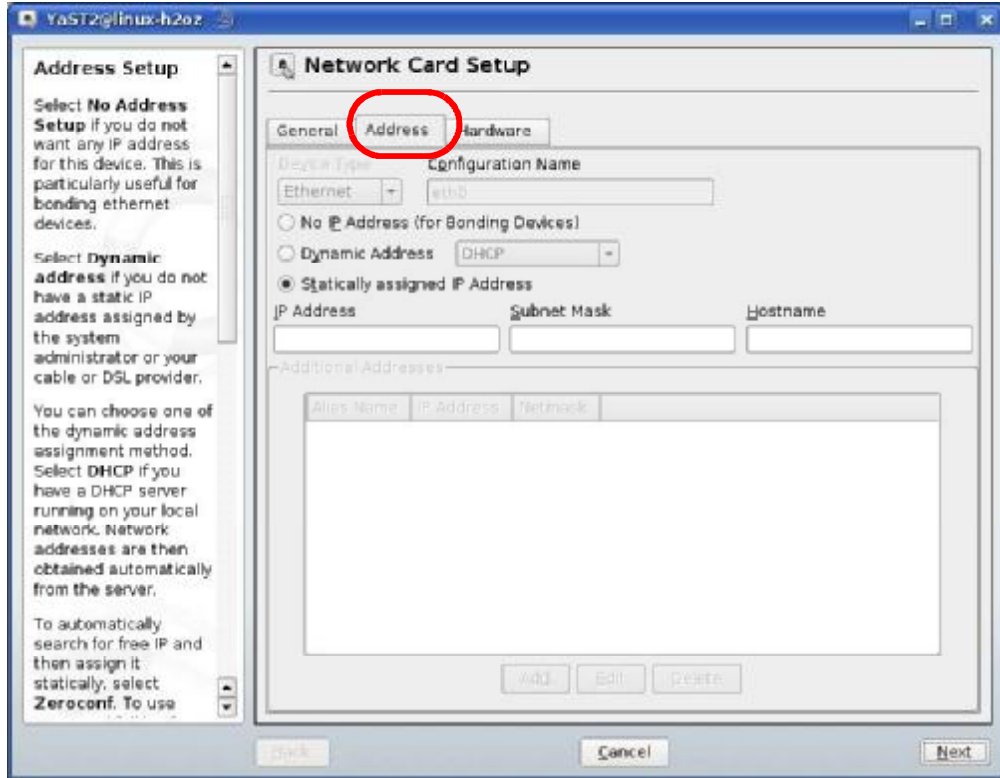
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 110 openSUSE 10.3: Network Settings



- 5 When the Network Card Setup window opens, click the Address tab

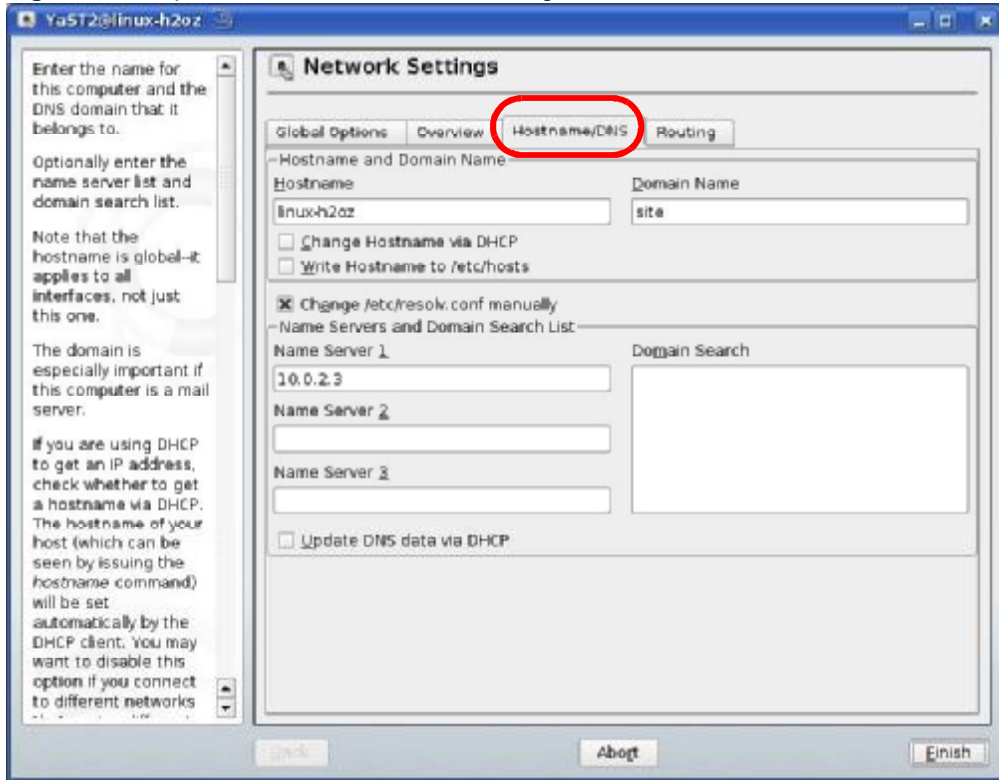
Figure 111 openSUSE 10.3: Network Card Setup



- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.

- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 112 openSUSE 10.3: Network Settings

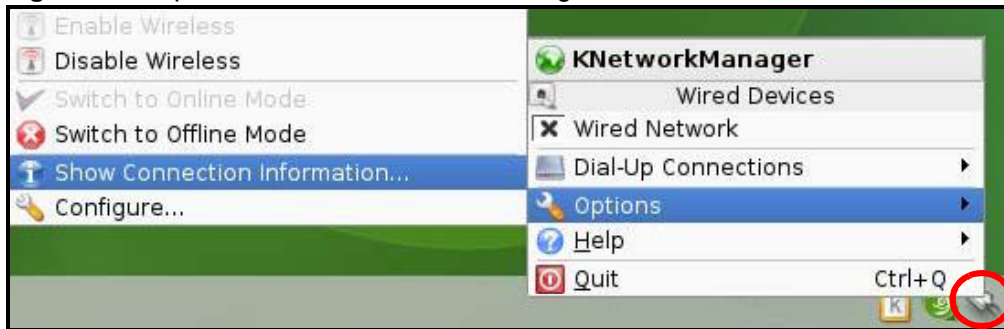


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

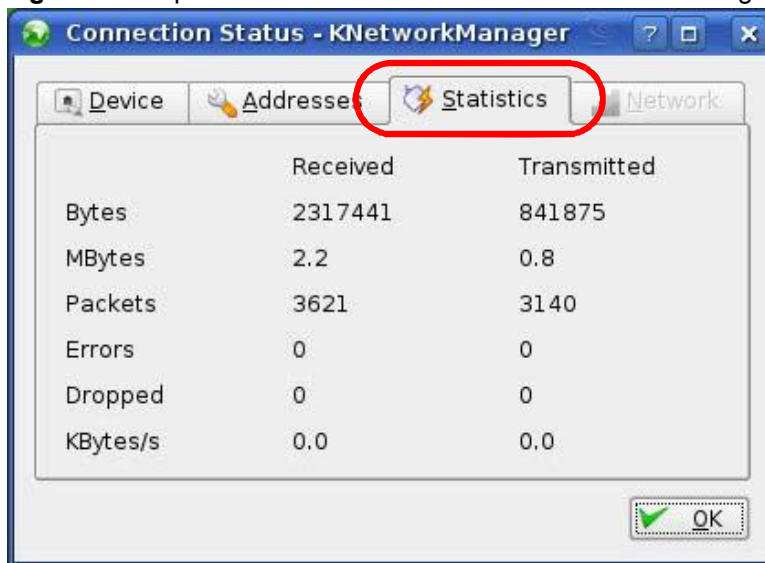
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 113 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics** tab to see if your connection is working properly.

Figure 114 openSUSE: Connection Status - KNetwork Manager



Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

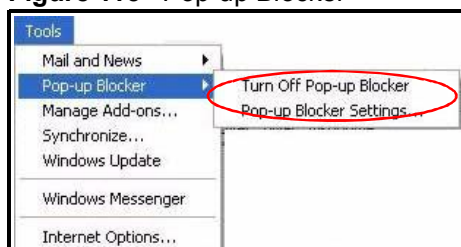
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

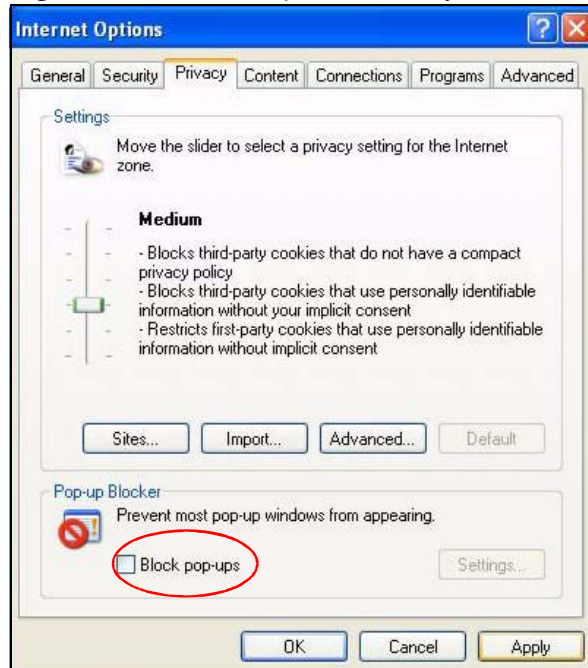
Figure 115 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 116 Internet Options: Privacy



- 3 Click **Apply** to save this setting.

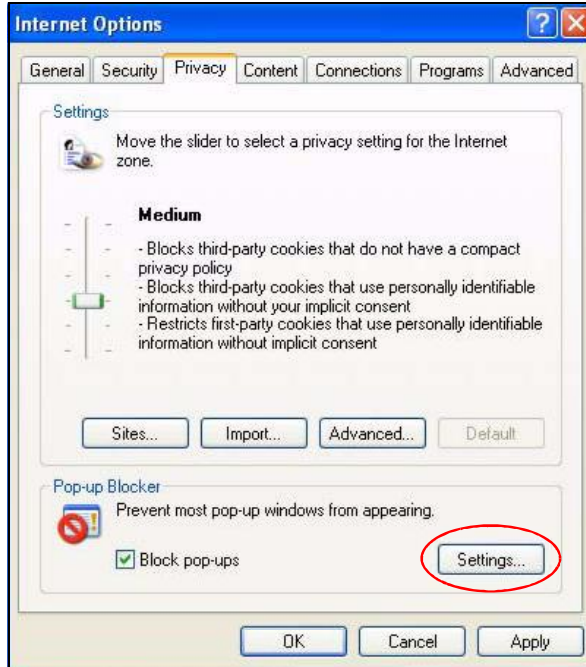
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 117 Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, <http://192.168.167.1>.

- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 118 Pop-up Blocker Settings



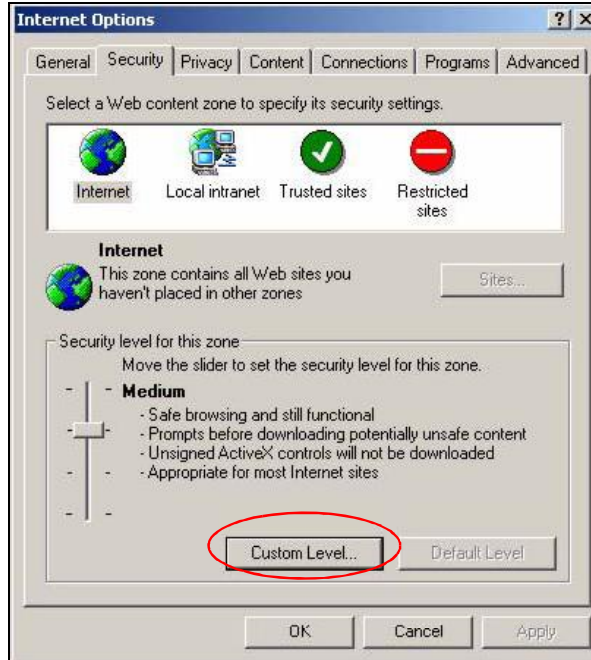
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

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

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

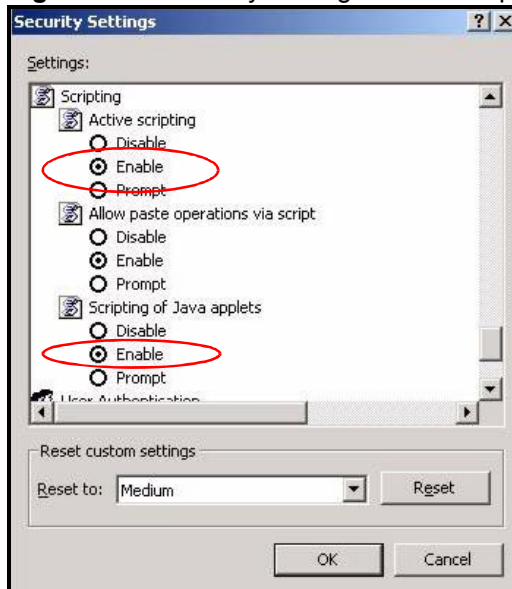
Figure 119 Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

Figure 120 Security Settings - Java Scripting

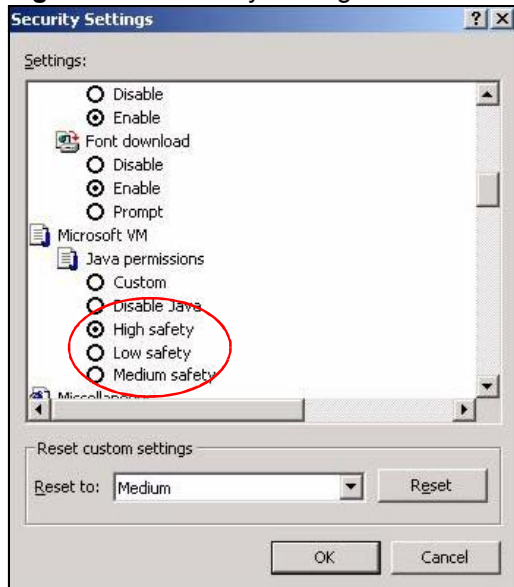


Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

Figure 121 Security Settings - Java

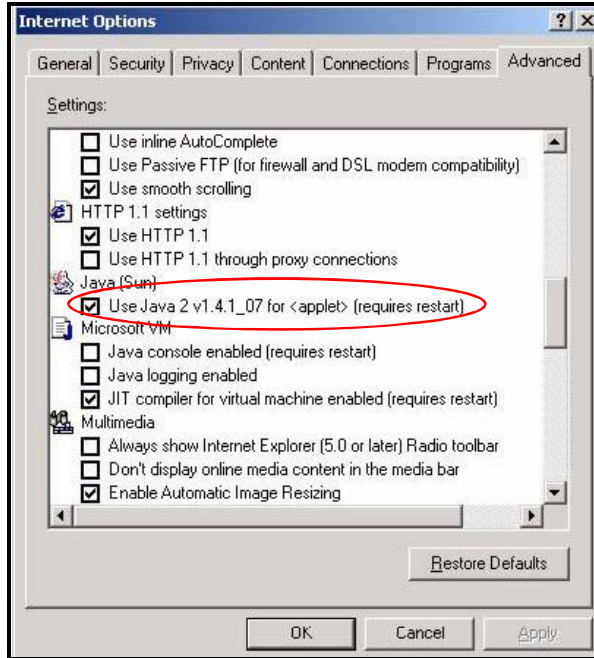


JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click OK to close the window.

Figure 122 Java (Sun)



Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

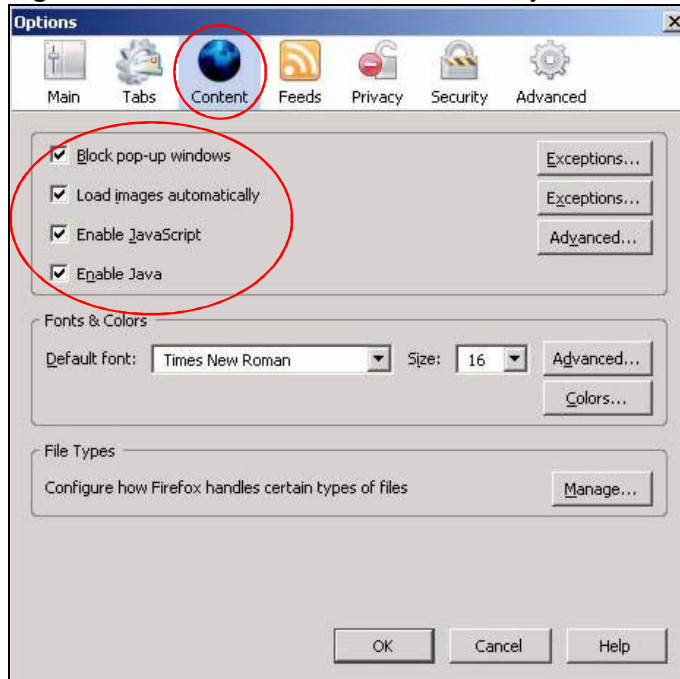
You can enable Java, Javascripts and pop-ups in one screen. Click Tools, then click Options in the screen that appears.

Figure 123 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 124 Mozilla Firefox Content Security



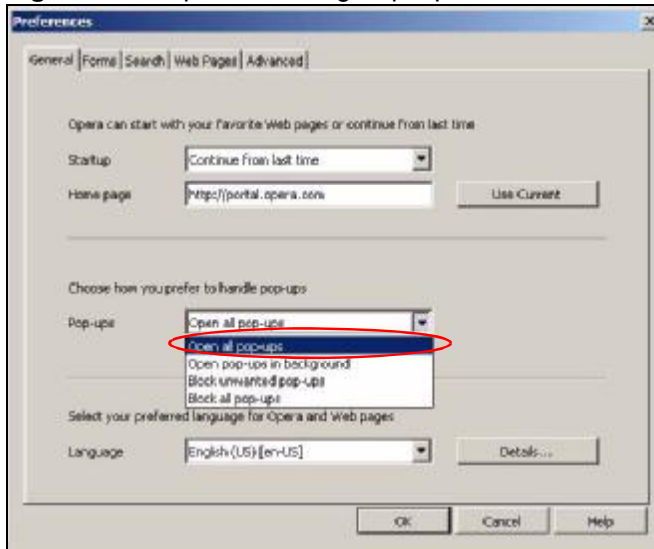
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

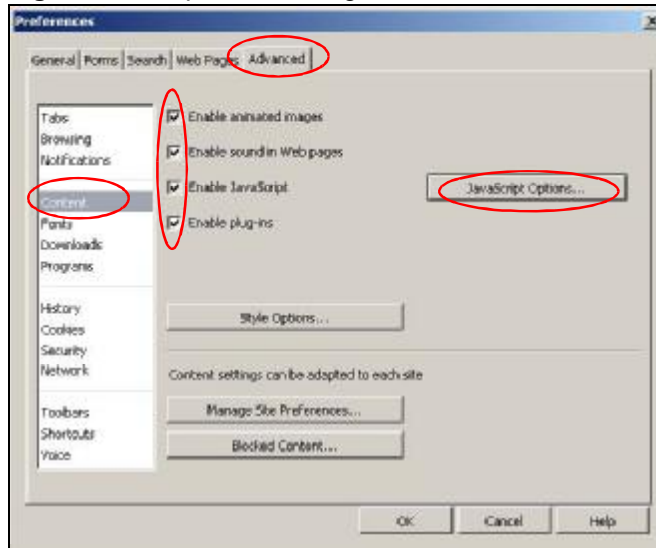
Figure 125 Opera: Allowing Pop-Ups



Enabling Java

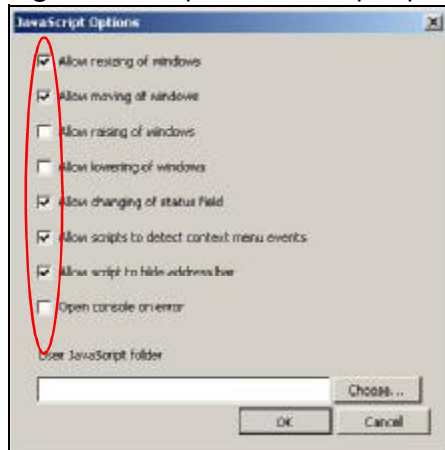
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 126 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 127 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

D

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

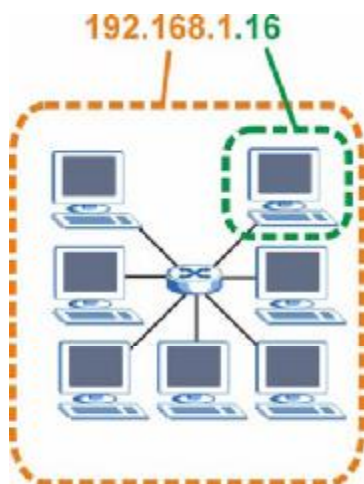
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 128 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 86 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 87 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 88 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 89 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

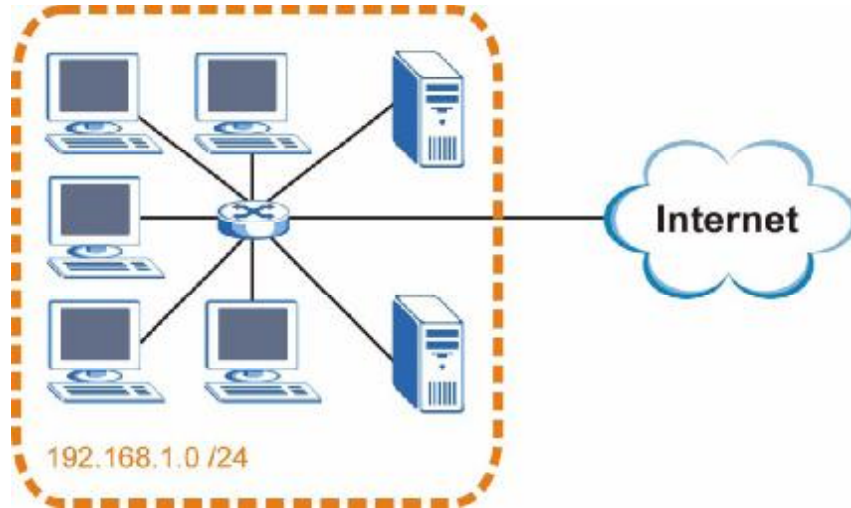
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 129 Subnetting Example: Before Subnetting

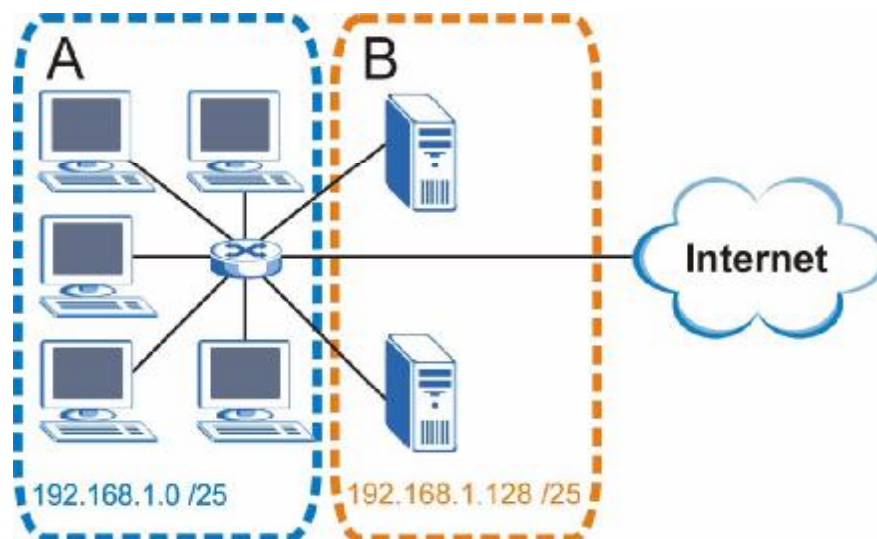


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, A and B.

Figure 130 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet A itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet A is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet B is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 90 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 91 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 92 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 93 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001. .	11000000
Subnet Mask (Binary)	11111111.11111111.11111111 .	11000000

Table 93 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 94 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 95 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 96 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the OX253P.

Once you have decided on the network number, pick an IP address for your OX253P that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your OX253P will compute the subnet mask automatically based on the IP address that

you entered. You don't need to change the subnet mask computed by the OX253P unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

IP Address Conflicts

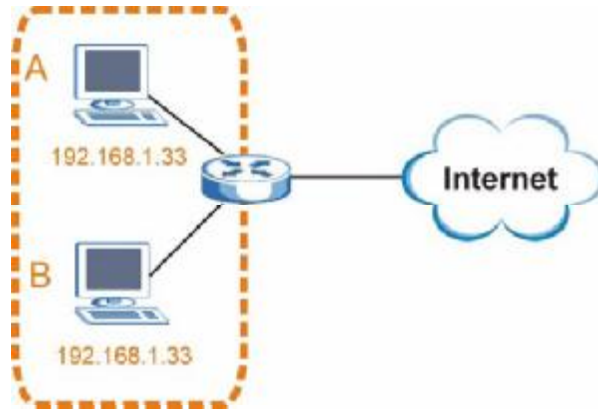
Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP

address to computer A or setting computer A to obtain an IP address automatically.

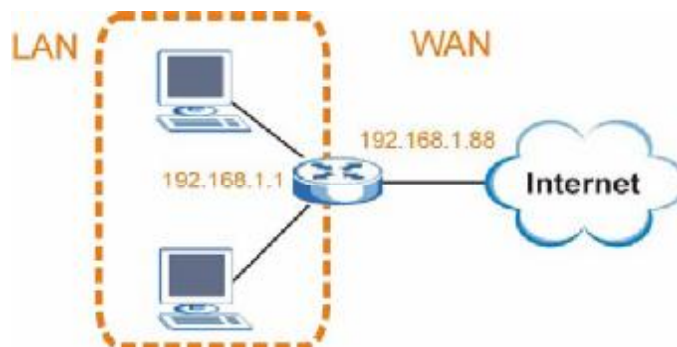
Figure 131 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

Figure 132 Conflicting Computer IP Addresses Example

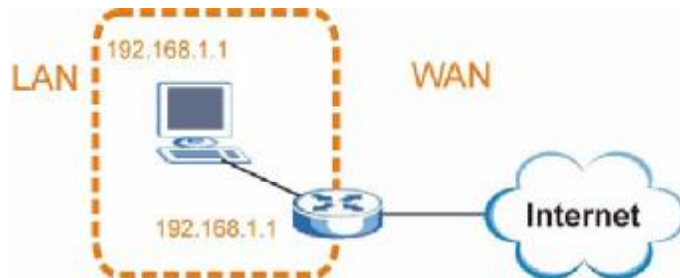


Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address.

The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 133 Conflicting Computer and Router IP Addresses Example






Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

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

Public key certificates can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon () somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

- Internet Explorer on [page 242](#)
- Firefox on [page 252](#)
- Opera on [page 258](#)
- Konqueror on [page 266](#)

Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

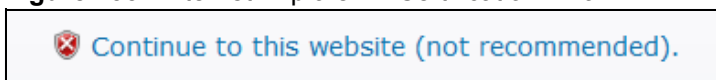
- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

Figure 134 Internet Explorer 7: Certification Error



- 2 Click **Continue to this website (not recommended)**.

Figure 135 Internet Explorer 7: Certification Error



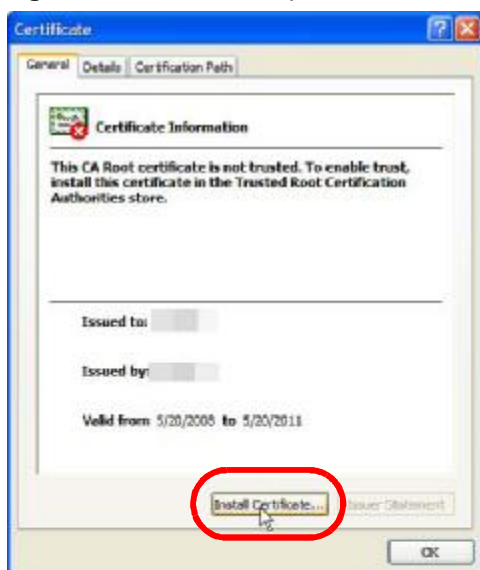
- 3 In the Address Bar, click Certificate Error > View certificates.

Figure 136 Internet Explorer 7: Certificate Error



- 4 In the Certificate dialog box, click Install Certificate.

Figure 137 Internet Explorer 7: Certificate



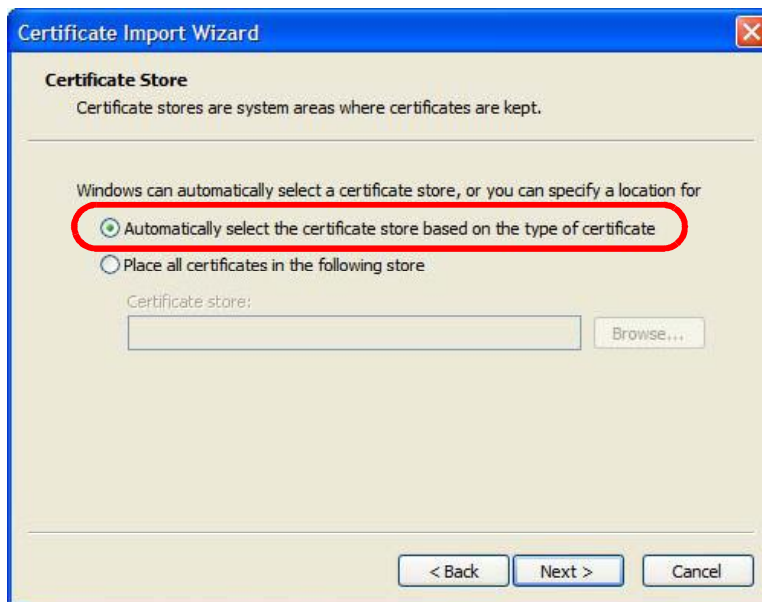
- 5 In the **Certificate Import Wizard**, click **Next**.

Figure 138 Internet Explorer 7: Certificate Import Wizard



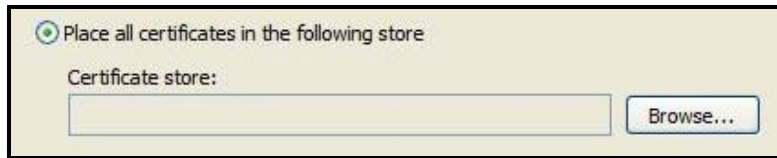
- 6 If you want Internet Explorer to **Automatically** select certificate store based on the type of certificate, click **Next** again and then go to step 9.

Figure 139 Internet Explorer 7: Certificate Import Wizard



- 7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

Figure 140 Internet Explorer 7: Certificate Import Wizard



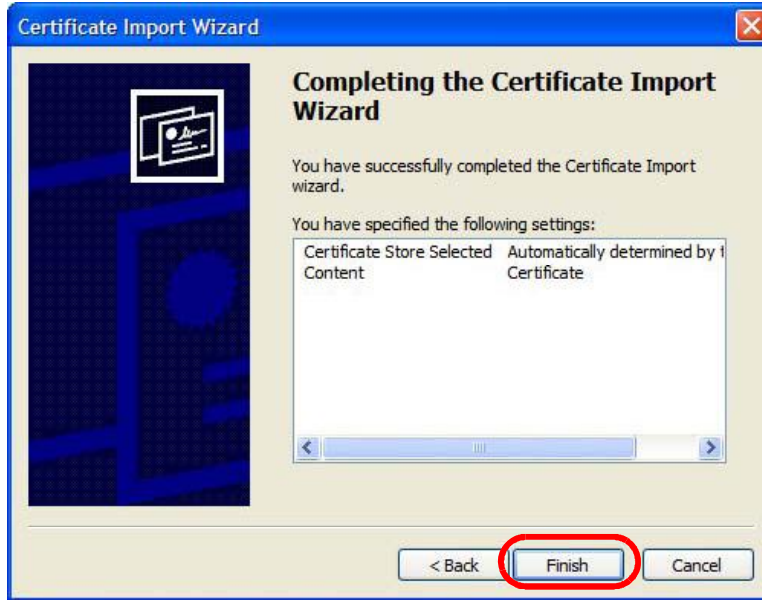
- 8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

Figure 141 Internet Explorer 7: Select Certificate Store



- 9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 142 Internet Explorer 7: Certificate Import Wizard



- 10 If you are presented with another **Security Warning**, click **Yes**.

Figure 143 Internet Explorer 7: Security Warning



- 11 Finally, click **OK** when presented with the successful certificate installation message.

Figure 144 Internet Explorer 7: Certificate Import Wizard



- 12 The next time you start Internet Explorer and go to a web configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

Figure 145 Internet Explorer 7: Website Identification



Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

- 1 Double-click the public key certificate file.

Figure 146 Internet Explorer 7: Public Key Certificate File



- 2 In the security warning dialog box, click **Open**.

Figure 147 Internet Explorer 7: Open File - Security Warning



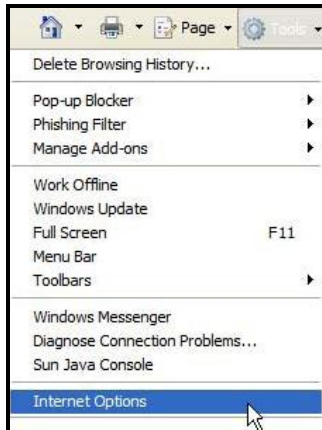
- 3 Refer to steps 4-12 in the Internet Explorer procedure beginning on [page 242](#) to complete the installation process.

Removing a Certificate in Internet Explorer

This section shows you how to remove a public key certificate in Internet Explorer 7.

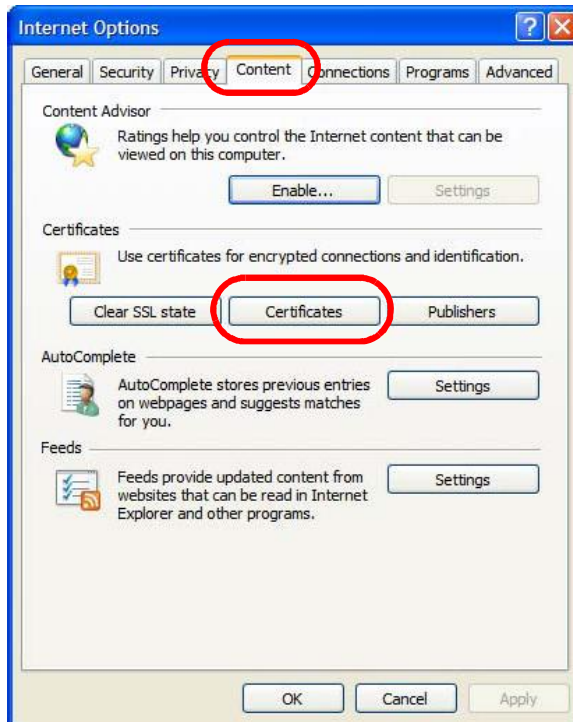
- 1 Open Internet Explorer and click **TOOLS > Internet Options**.

Figure 148 Internet Explorer 7: Tools Menu



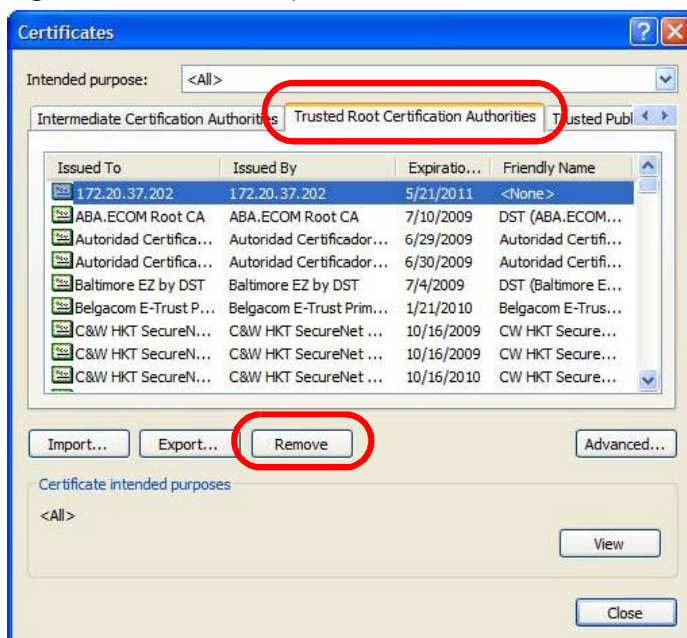
- 2 In the **Internet Options** dialog box, click **Content > Certificates**.

Figure 149 Internet Explorer 7: Internet Options



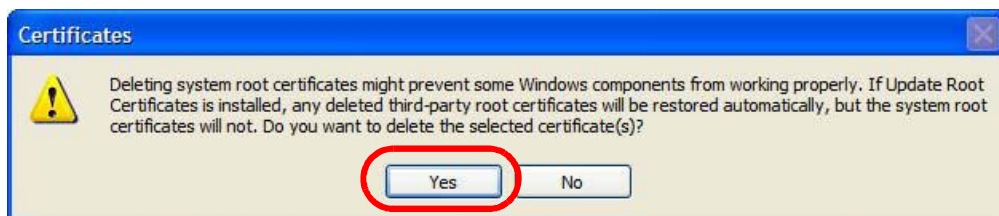
- In the Certificates dialog box, click the Trusted Root Certificates Authorities tab, select the certificate that you want to delete, and then click Remove.

Figure 150 Internet Explorer 7: Certificates



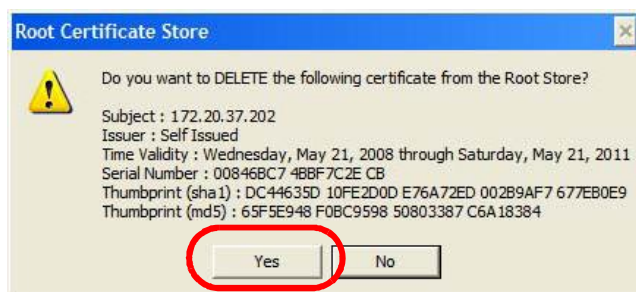
- In the Certificates confirmation, click Yes.

Figure 151 Internet Explorer 7: Certificates



- In the Root Certificate Store dialog box, click Yes.

Figure 152 Internet Explorer 7: Root Certificate Store



- 6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Select **Accept this certificate permanently** and click **OK**.

Figure 153 Firefox 2: Website Certified by an Unknown Authority



- 3 The certificate is stored and you can now connect securely to the web configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info > Security** window to view the web page's security information.

Figure 154 Firefox 2: Page Info

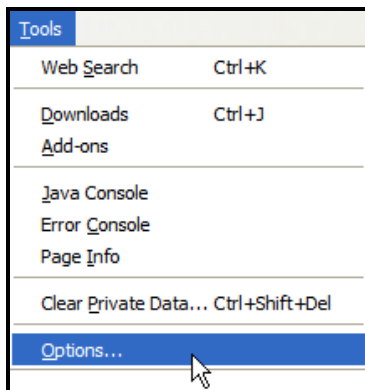


Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

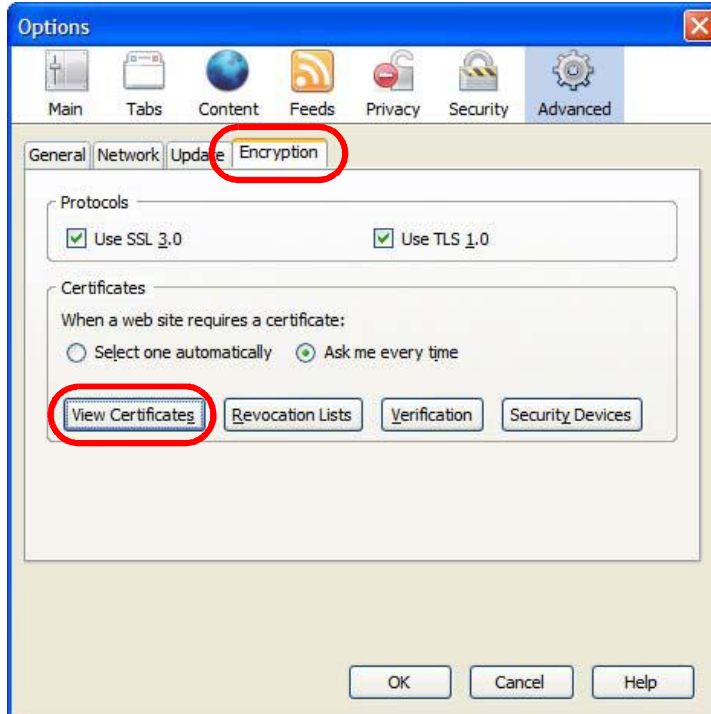
- 1 Open Firefox and click **TOOLS > Options**.

Figure 155 Firefox 2: Tools Menu



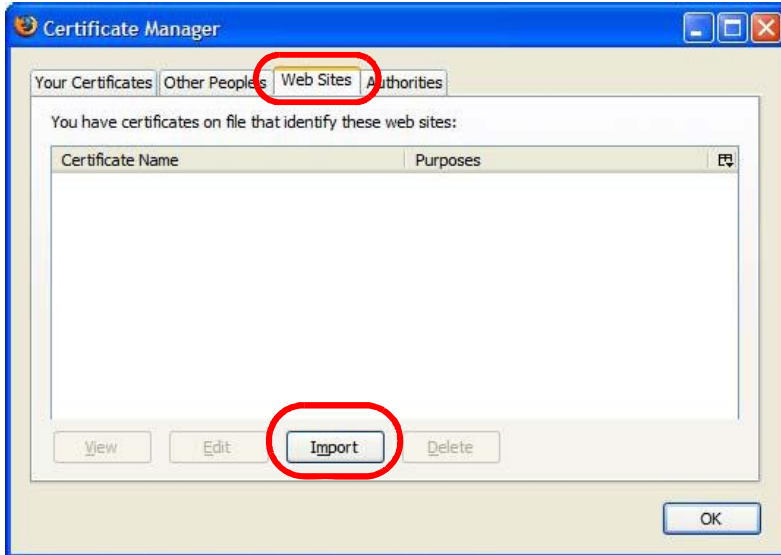
- 2 In the Options dialog box, click **ADVANCED > Encryption > View Certificates**.

Figure 156 Firefox 2: Options



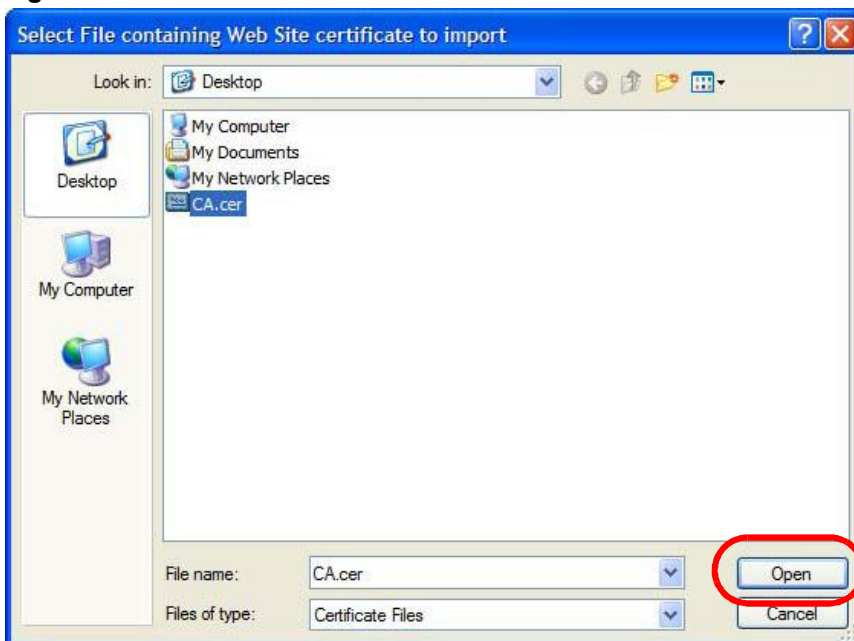
- 3 In the Certificate Manager dialog box, click **Web Sites > Import**.

Figure 157 Firefox 2: Certificate Manager



- 4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

Figure 158 Firefox 2: Select File



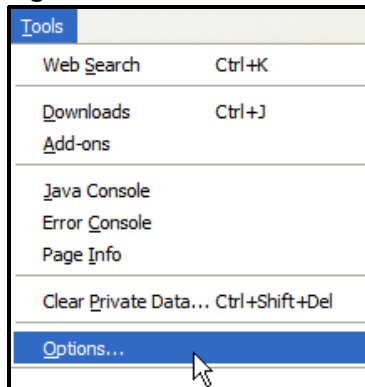
- 5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

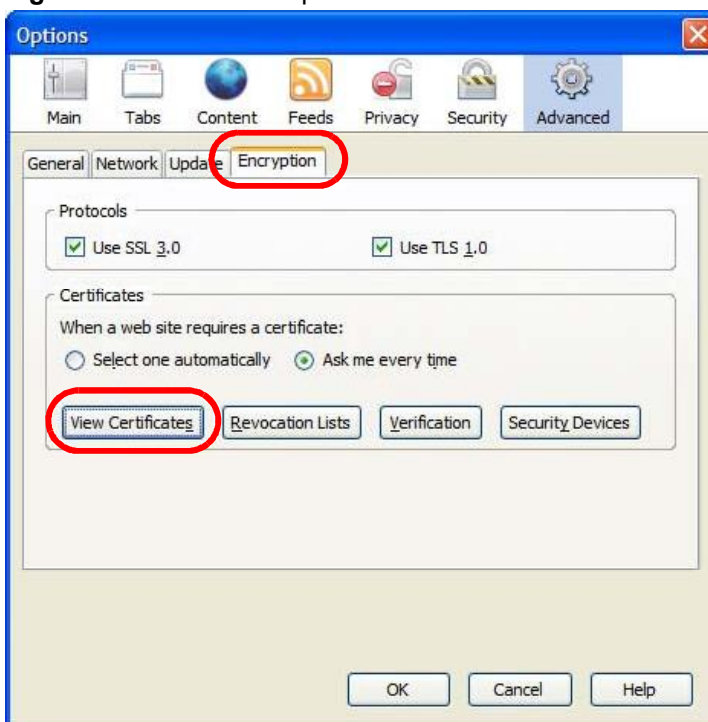
- 1 Open Firefox and click **TOOLS > Options**.

Figure 159 Firefox 2: Tools Menu



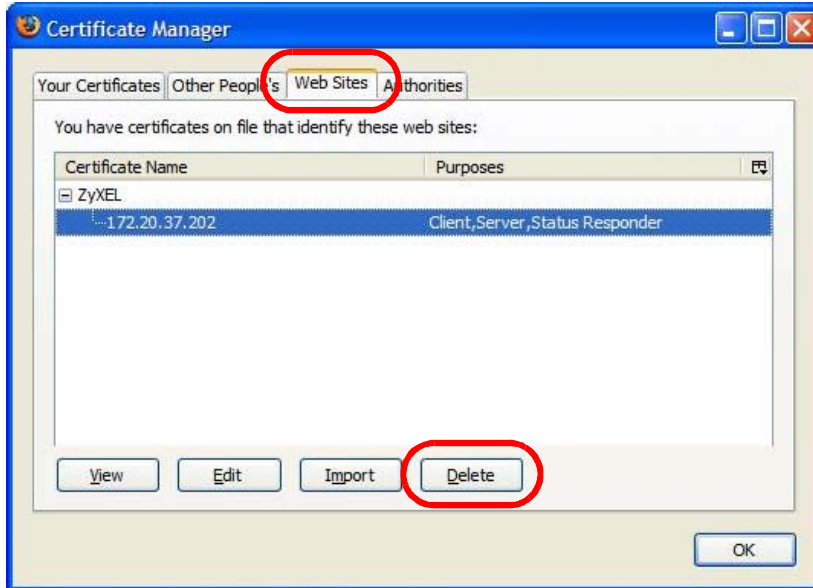
- 2 In the Options dialog box, click **ADVANCED > Encryption > View Certificates**.

Figure 160 Firefox 2: Options



- 3 In the Certificate Manager dialog box, select the Web Sites tab, select the certificate that you want to remove, and then click Delete.

Figure 161 Firefox 2: Certificate Manager



- 4 In the Delete Web Site Certificates dialog box, click OK.

Figure 162 Firefox 2: Delete Web Site Certificates



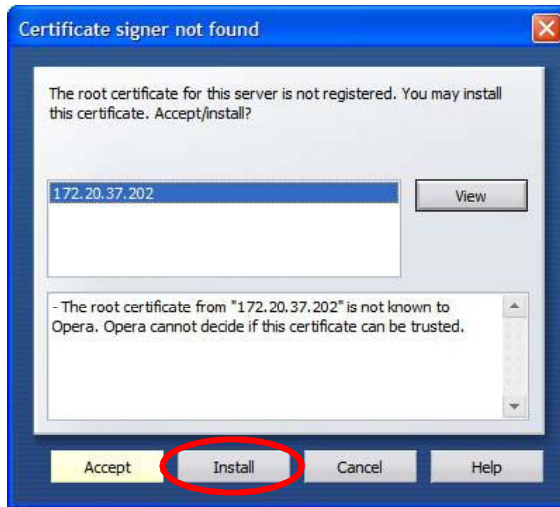
- 5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

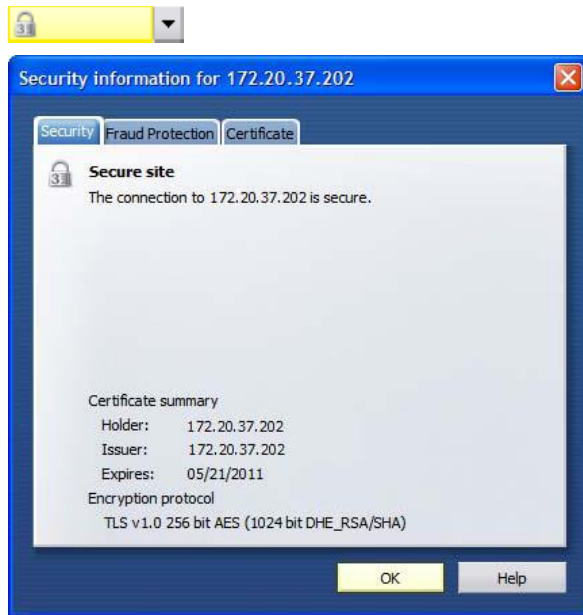
- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Click **Install** to accept the certificate.

Figure 163 Opera 9: Certificate signer not found



- 3 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Figure 164 Opera 9: Security information

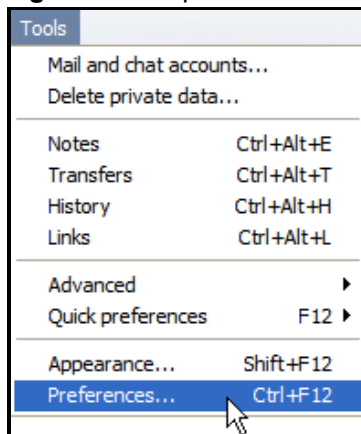


Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

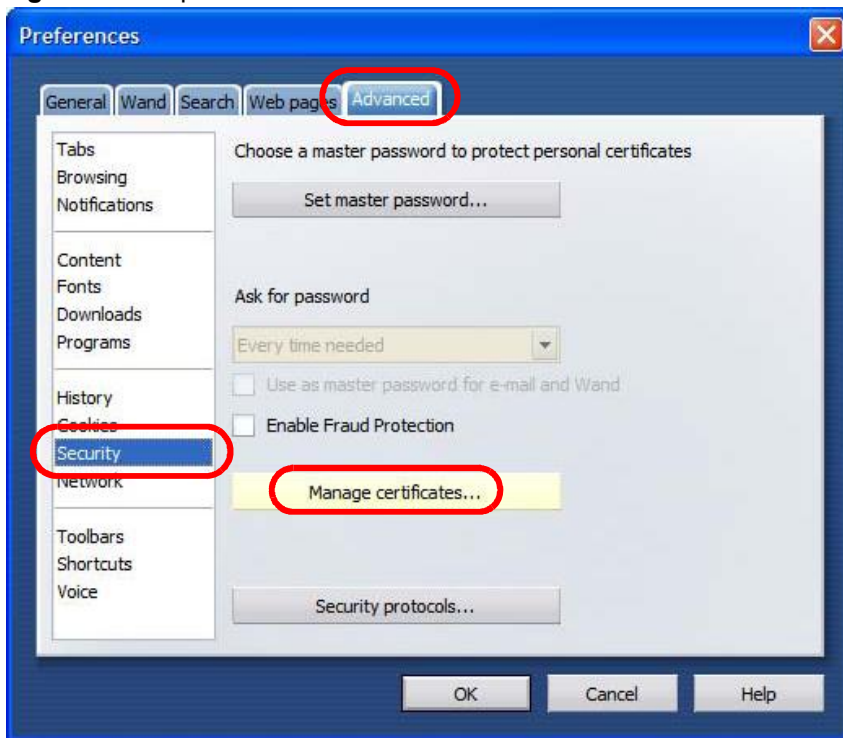
- 1 Open Opera and click **TOOLS > Preferences**.

Figure 165 Opera 9: Tools Menu



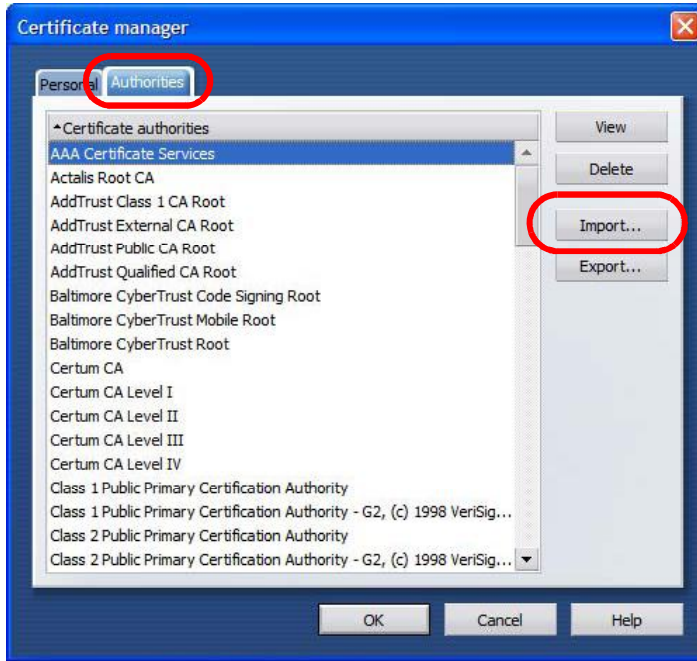
- 2 In Preferences, click **ADVANCED** > **Security** > **Manage certificates**.

Figure 166 Opera 9: Preferences



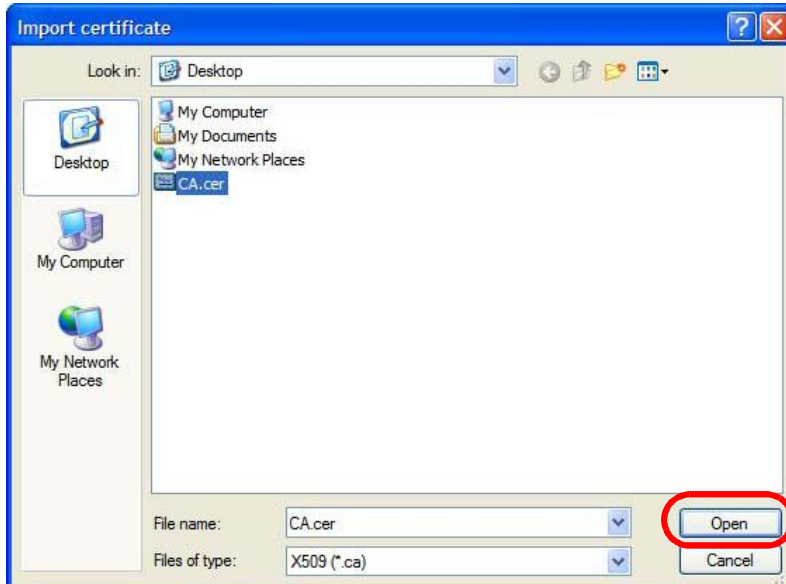
- 3 In the Certificates Manager, click Authorities > Import.

Figure 167 Opera 9: Certificate manager



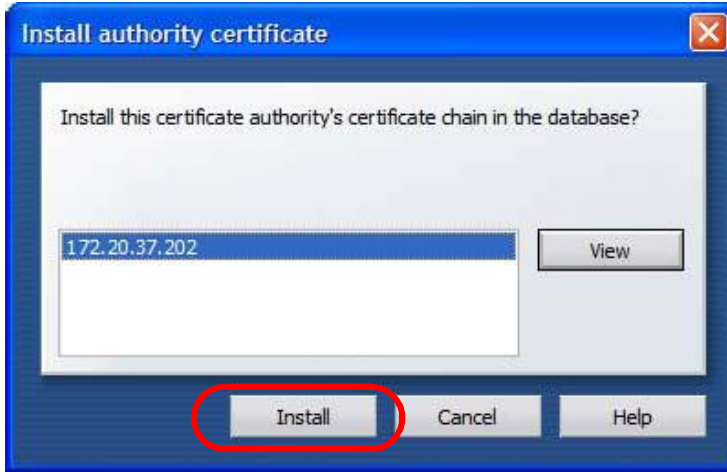
- 4 Use the Import certificate dialog box to locate the certificate and then click Open.

Figure 168 Opera 9: Import certificate



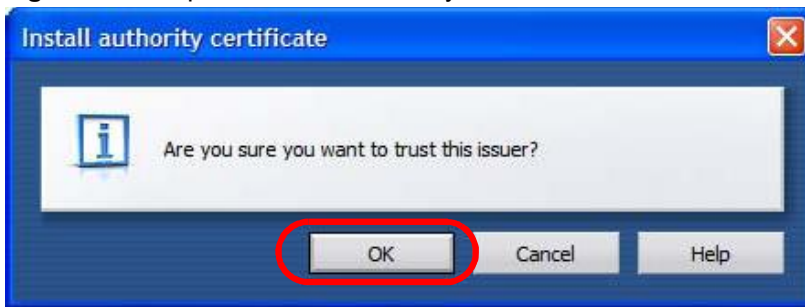
- 5 In the **Install authority certificate** dialog box, click **Install**.

Figure 169 Opera 9: Install authority certificate



- 6 Next, click **OK**.

Figure 170 Opera 9: Install authority certificate



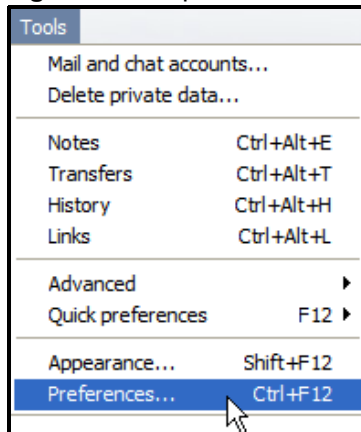
- 7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

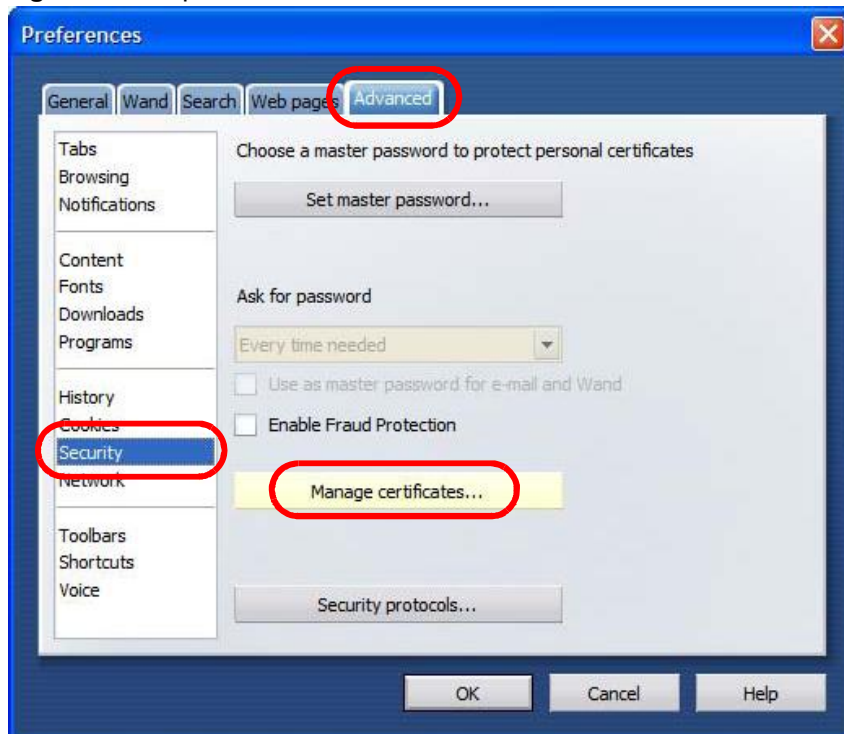
- 1 Open Opera and click **TOOLS > Preferences**.

Figure 171 Opera 9: Tools Menu



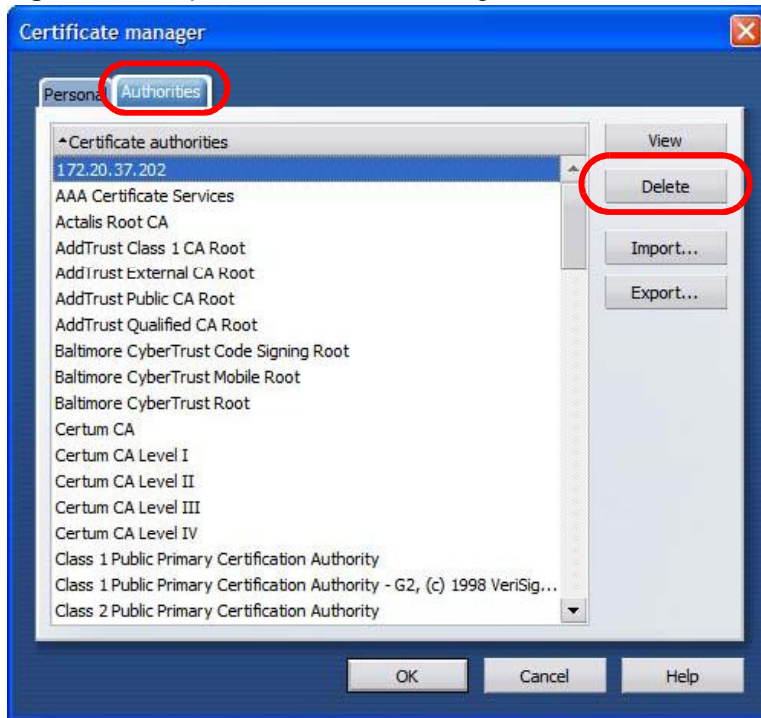
- 2 In Preferences, **ADVANCED > Security > Manage certificates**.

Figure 172 Opera 9: Preferences



- 3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 173 Opera 9: Certificate manager



- 4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

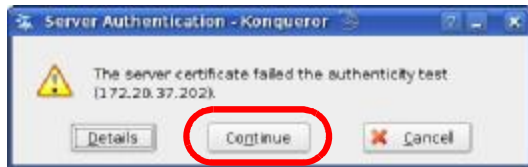
Note: There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Click **Continue**.

Figure 174 Konqueror 3.5: Server Authentication



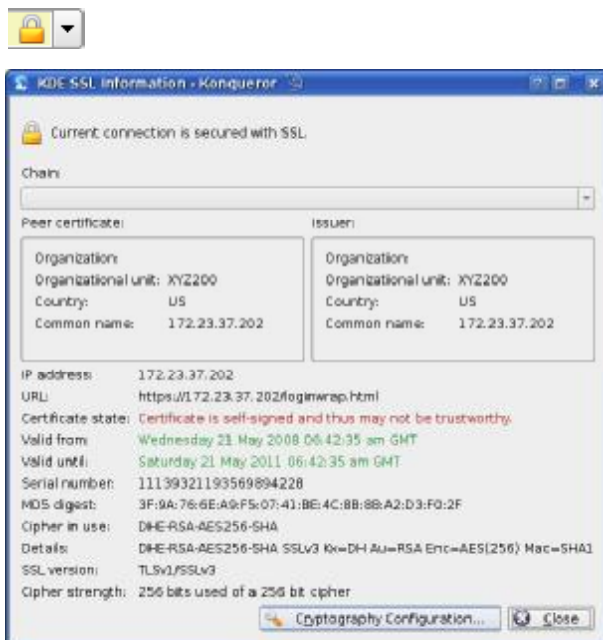
- 3 Click **Forever** when prompted to accept the certificate.

Figure 175 Konqueror 3.5: Server Authentication



- 4 Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

Figure 176 Konqueror 3.5: KDE SSL Information



Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

- 1 Double-click the public key certificate file.

Figure 177 Konqueror 3.5: Public Key Certificate File



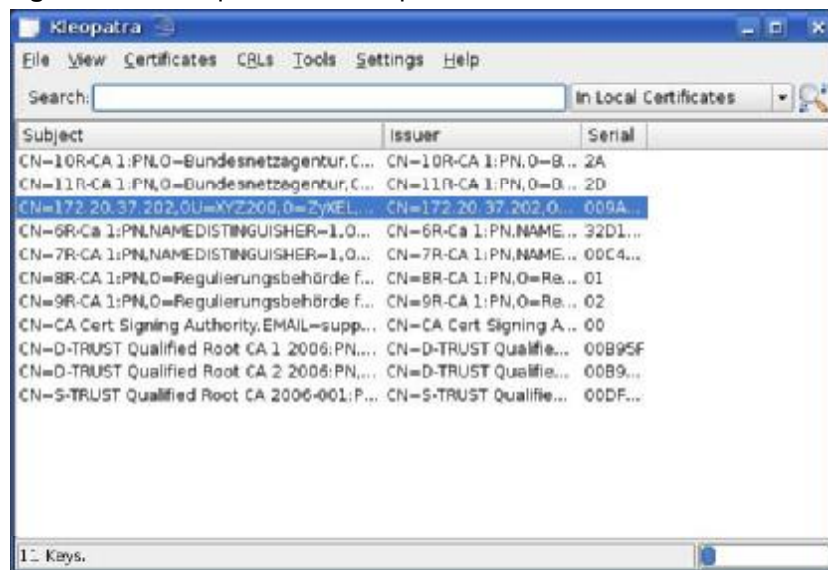
- 2 In the Certificate Import Result - Kleopatra dialog box, click OK.

Figure 178 Konqueror 3.5: Certificate Import Result



The public key certificate appears in the KDE certificate manager, Kleopatra.

Figure 179 Konqueror 3.5: Kleopatra



- 3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

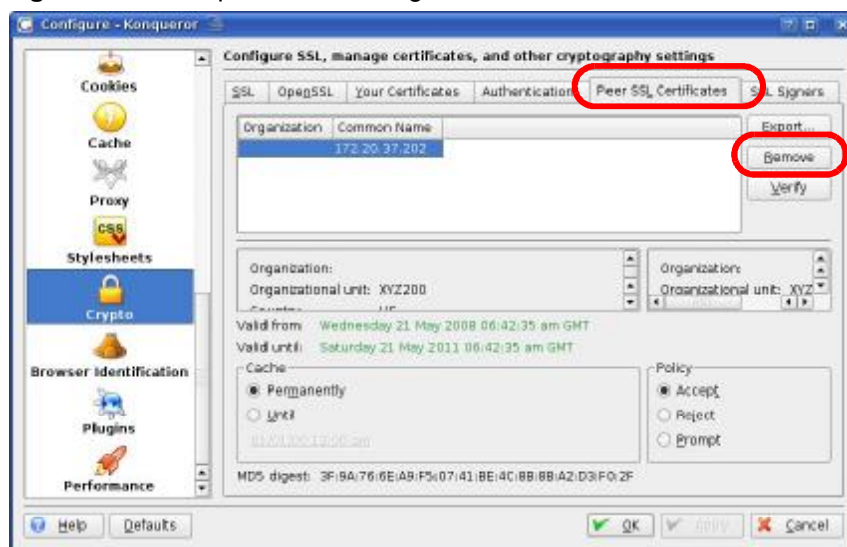
- 1 Open Konqueror and click **Settings > Configure Konqueror**.

Figure 180 Konqueror 3.5: Settings Menu



- 2 In the **Configure** dialog box, select **Crypto**.
- 3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

Figure 181 Konqueror 3.5: Configure



- 4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.

Common Services

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

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is TCP/UDP, then the service uses the same port number with TCP and UDP. If this is USER-DEFINED, the Port(s) is the IP protocol number, not the port number.
- **Port(s):** This value depends on the Protocol. Please refer to RFC 1700 for further information about port numbers.
 - If the Protocol is TCP, UDP, or TCP/UDP, this is the IP port number.
 - If the Protocol is USER, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 97 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.

Table 97 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 97 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 97 Commonly Used Services (continued)

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

Index

Numbers

16QAM [171](#)

A

AAA [67](#)

accounting server
see AAA

ACS, see Auto Configuration Server

activity [67](#)

Advanced Encryption Standard
see AES

AES [187](#)

ALG [85](#)

alternative subnet mask notation [232](#)

application

CWMP-TR-069 [142](#)

Application Layer Gateway
see ALG

authentication [31, 67, 69, 185](#)

inner [188](#)

key

server [67](#)

types [188](#)

authorization [185](#)

request and reply [187](#)

server [67](#)

Auto Configuration Server [142](#)

B

base station
see BS

BS [65–66](#)
links [66](#)

buzzer [74](#)

buzzer and ODU LEDs [75](#)

buzzer and RSSI [75](#)

C

CA [97, 114](#)

and certificates [114](#)

CBC-MAC [187](#)

CCMP [185, 187](#)

cell [65](#)

Certificate Management Protocol (CMP) [102](#)

Certificate Revocation List (CRL) [114](#)

certificates [97, 185](#)

advantages [115](#)

and CA [114](#)

certification path [105, 111, 114](#)

expired [114](#)

factory-default [115](#)

file formats [115](#)

fingerprints [106, 112](#)

importing [99](#)

not used for encryption [114](#)

revoked [114](#)

self-signed [101](#)

serial number [105, 111](#)

storage space [98](#)

thumbprint algorithms [117](#)

thumbprints [117](#)

used for authentication [114](#)

verification [187](#)

verifying fingerprints [116](#)

certification

authority, see CA

requests [97, 101, 102](#)

chaining [187](#)

chaining message authentication
see CCMP

CMAC

see MAC

counter mode

see CCMP

coverage area [65](#)
cryptography [185](#)
CWMP-TR-069 [142](#)

D

data [185–187](#)
 decryption [185](#)
 encryption [185](#)
 flow [187](#)
DHCP [54, 88, 90](#)
 client [88](#)
 server [54](#)
diameter [67](#)
digital ID [185](#)
DL frequency [73, 74](#)
domain name [88](#)
download frequency
 see DL frequency
dynamic DNS [90](#)
Dynamic Host Configuration Protocol
 see DHCP

E

EAP [67](#)
encryption [185–187](#)
 traffic [187](#)
Ethernet
 encapsulation [78](#)
Extensible Authorization Protocol
 see EAP
Extensible Markup Language, see XML

F

firewall [119, 124, 125](#)
frequency
 band [74](#)
 ranges [73, 74](#)
 scanning [74](#)
FTP [90, 134](#)

restrictions [134](#)

I

IANA [238](#)
identity [67, 185](#)
idle timeout [134](#)
IEEE 802.16 [65, 185](#)
IEEE 802.16e [65](#)
inner authentication [188](#)
Internet
 access [67](#)
Internet Assigned Numbers Authority
 see IANA [238](#)
interoperability [65](#)

K

key [31, 69, 185](#)
 request and reply [187](#)

M

MAC [187](#)
MAN [65](#)
Management Information Base (MIB) [138](#)
manual site survey [73, 74](#)
Message Authentication Code
 see MAC
message integrity [187](#)
Metropolitan Area Network
 see MAN
microwave [65, 66](#)
mobile station
 see MS
modulation [171](#)
MS [66](#)
My Certificates [98](#)
 see also certificates

N

- NAT [237](#)
 - and remote management [134](#)
 - server sets [78](#)
- network
 - activity [67](#)
 - services [67](#)

O

- ODU LEDs and buzzer [75](#)

P

- pattern-spotting [187](#)
- PKMv2 [31](#), [67](#), [69](#), [185](#), [188](#)
- plain text encryption [187](#)
- Privacy Key Management
 - see PKM
- private key [185](#)
- public certificate [187](#)
- public key [31](#), [69](#), [185](#)
- Public-Key Infrastructure (PKI) [114](#)
- public-private key pairs [97](#), [114](#)

Q

- QoS [145](#)
- QPSK [171](#)
- Quality of Service, see QoS

R

- radio frequency of WiMAX [66](#)
- RADIUS [67](#), [186](#)
 - Message Types [186](#)
 - Messages [186](#)
 - Shared Secret Key [186](#)
- related documentation [3](#)

- remote management and NAT [134](#)
- remote management limitations [134](#)
- Remote Procedure Call [142](#)
- RFC 2510. See Certificate Management Protocol.
- RSSI and buzzer [75](#)

S

- safety warnings [6](#)
- secure communication [31](#), [69](#), [185](#)
- secure connection [67](#)
- security [185](#)
- security association [187](#)
 - see SA
- services [67](#)
- Simple Certificate Enrollment Protocol (SCEP) [102](#)
- SIP
 - ALG [85](#)
 - Application Layer Gateway, see ALG
- SNMP [135](#)
 - manager [137](#)
- spectrum range of WiMAX [66](#)
- SS [65](#), [66](#)
- stateful inspection [124](#)
- subnet [229](#)
 - mask [230](#)
- subnetting [232](#)
- subscriber station
 - see SS
- syntax conventions [4](#)
- system timeout [134](#)

T

- tampering
- TCP/IP configuration [54](#)
- TEK [187](#)
- TFTP restrictions [134](#)
- TLS [31](#), [69](#), [185](#)
- transport encryption key

see TEK
transport layer security
 see TLS
triangle route
 problem [125](#)
 solutions [126](#)
trigger port forwarding
 process [84](#)
TTLS [31](#), [69](#), [185](#), [188](#)
tunneled TLS
 see TTLS

X

XML [142](#)

U

unauthorized device [185](#)
user authentication [185](#)
user name [91](#)

V

verification [187](#)

W

WiMAX
 radio frequency [66](#)
 security [187](#)
 spectrum range [66](#)
 WiMAX Forum [65](#)
Wireless Interoperability for Microwave Access
 see WiMAX
Wireless Metropolitan Area Network
 see MAN
wireless network
 access [65](#)
 standard [65](#)
wireless security [185](#)
wizard setup [29](#)

