15.4 Technical Reference

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

15.4.1 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.

15.4.2 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.

15.4.3 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 MAX-207HW2R’s LAN IP address), the "triangle route" (also called asymmetrical route) problem may occur. The steps below describe the "triangle route" problem.

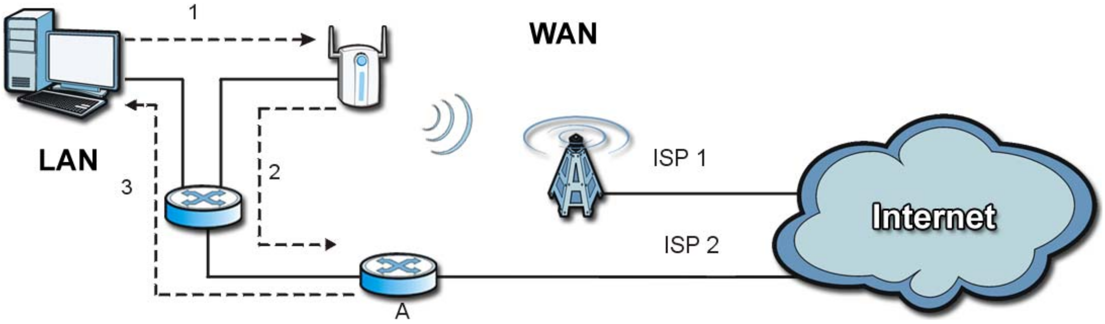
1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

2 The MAX-207HW2R 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 MAX-207HW2R.

As a result, the MAX-207HW2R resets the connection, as the connection has not been acknowledged.

Figure 68 "Triangle Route" Problem



15.4.3.1 Solving the "Triangle Route" Problem

If you have the MAX-207HW2R allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the MAX-207HW2R 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 MAX-207HW2R supports up to three logical LAN interfaces with the MAX-207HW2R 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 MAX-207HW2R to your LAN. The following steps describe such a scenario.

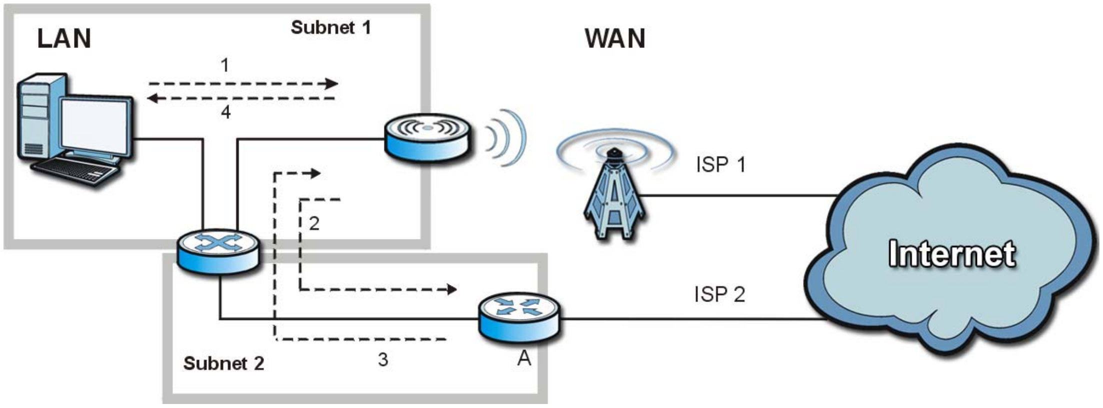
1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

2 The MAX-207HW2R reroutes the packet to Gateway A, which is in Subnet 2.

3 The reply from the WAN goes to the MAX-207HW2R.

4 The MAX-207HW2R then sends it to the computer on the LAN in Subnet 1.

Figure 69 IP Alias



16

Content Filter

16.1 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 MAX-207HW2R can block web features such as ActiveX controls, Java applets, cookies and disable web proxies. The MAX-207HW2R also allows you to define time periods and days during which the MAX-207HW2R performs content filtering.

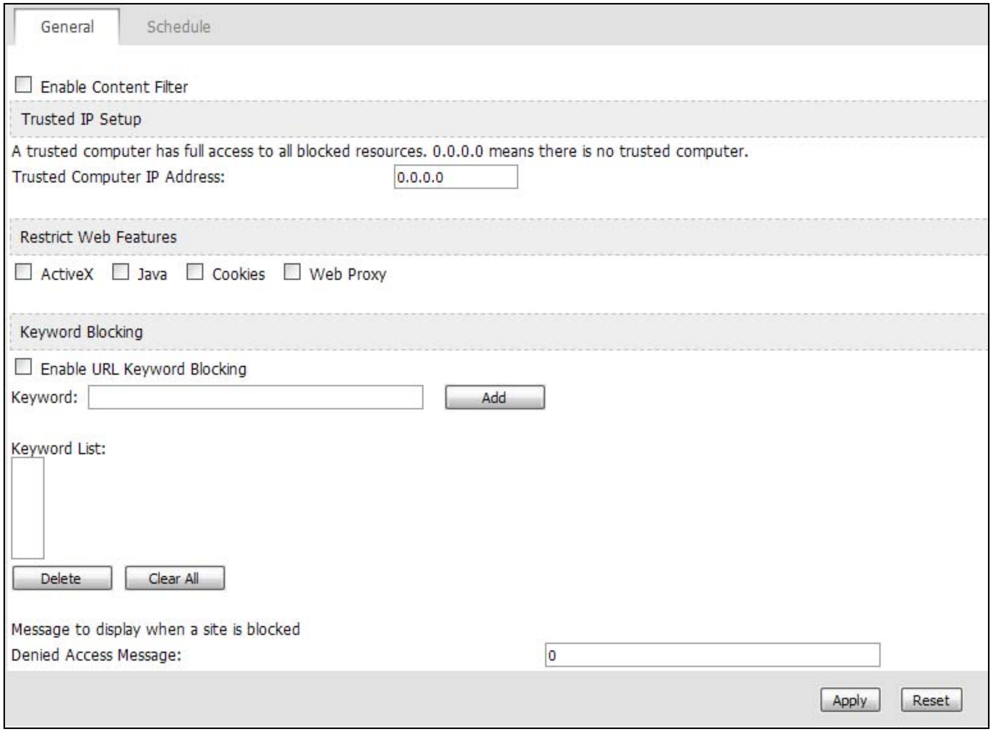
16.1.1 What You Can Do in This Chapter

- The **General** screen (Section 16.2 on page 156) 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 16.3 on page 158) lets you schedule content filtering.

16.2 Filter

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

Figure 70 TOOLS > Content Filter > General



□ Enable Content Filter

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: 0.0.0.0

Restrict Web Features

□ ActiveX □ Java □ Cookies □ Web Proxy

Keyword Blocking

□ Enable URL Keyword Blocking

Keyword:

Keyword List:

Message to display when a site is blocked

Denied Access Message: 0

The following table describes the labels in this screen.

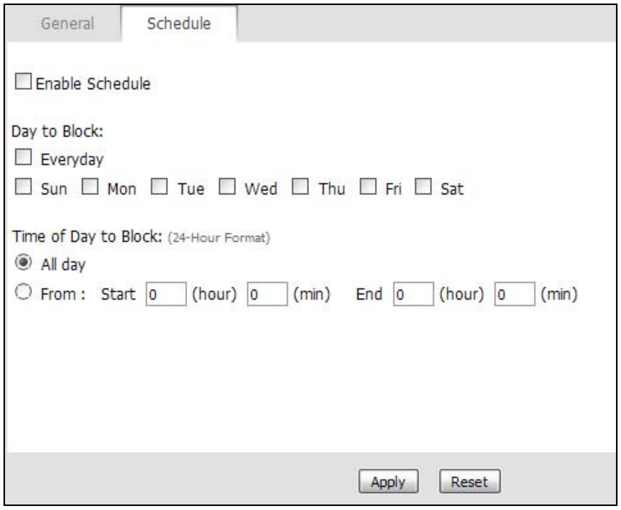
Table 62 TOOLS > Content Filter > General

LABEL	DESCRIPTION
Enable Content Filter	
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 MAX-207HW2R 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 MAX-207HW2R's content filter feature blocks access to a web site.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

16.3 Schedule

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

Figure 71 TOOLS > Content Filter > Schedule



□ Enable Schedule

Day to Block:

□ Everyday

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

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

● All day

○ From : Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

The following table describes the labels in this screen.

Table 63 TOOLS > Content Filter > Schedule

LABEL	DESCRIPTION
Enable Schedule	Select this if you want to enable the schedule.
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.

17

The Password Setup Screen

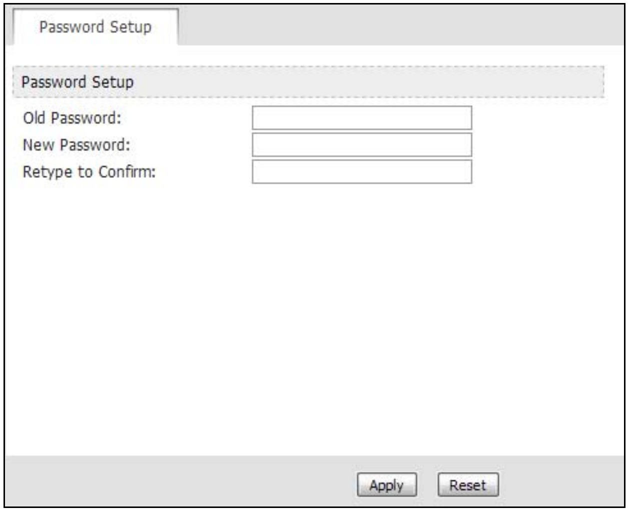
17.1 Overview

The default administrator password is 1234. Use this screen to change it.

17.2 Password Setup

Click **TOOLS > Password Setup** to change the administrator password.

Figure 72 TOOLS > Password Setup



The following table describes the labels in this screen.

Table 64 TOOLS > Password Setup

LABEL	DESCRIPTION
Password Setup	
Old Password	Enter the current password you use to access the MAX-207HW2R.
New Password	Enter the new password for the MAX-207HW2R. You can use up to 30 characters. As you type the password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Enter the new password again.

Table 64 TOOLS > Password Setup

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

The Status Screen

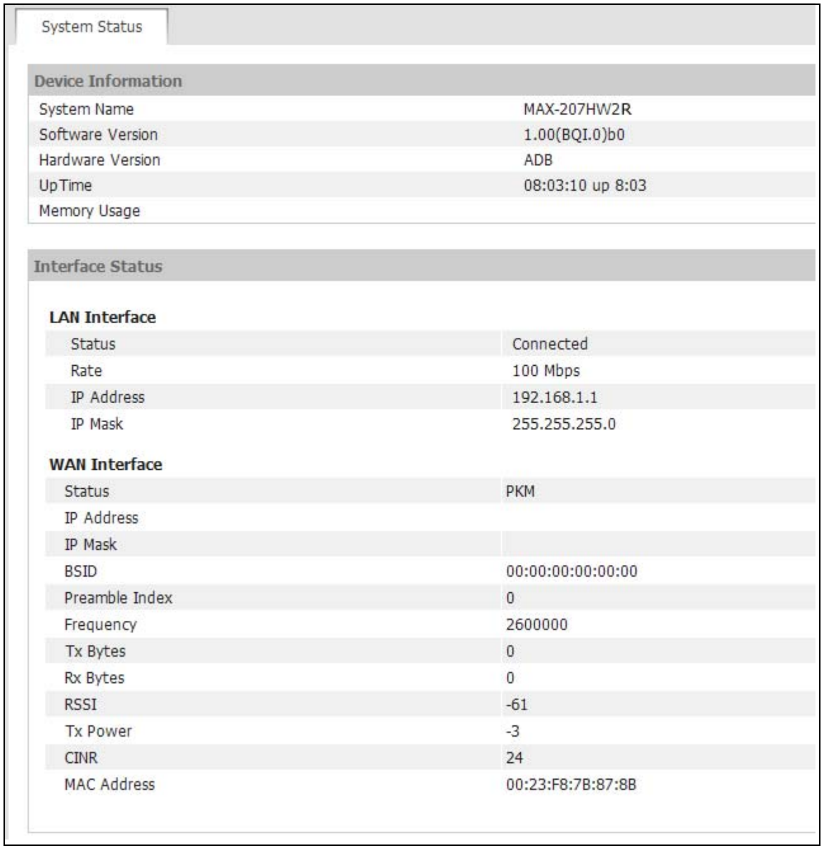
18.1 Overview

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

18.2 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, and interfaces (LAN and WAN).

Figure 73 Status



Device Information

System Name	MAX-207HW2R
Software Version	1.00(BQI.0)b0
Hardware Version	ADB
UpTime	08:03:10 up 8:03
Memory Usage	

Interface Status

LAN Interface

Status	Connected
Rate	100 Mbps
IP Address	192.168.1.1
IP Mask	255.255.255.0

WAN Interface

Status	PKM
IP Address	
IP Mask	
BSID	00:00:00:00:00:00
Preamble Index	0
Frequency	2600000
Tx Bytes	0
Rx Bytes	0
RSSI	-61
Tx Power	-3
CINR	24
MAC Address	00:23:F8:7B:87:8B

The following tables describe the labels in this screen.

Table 65 Status

LABEL	DESCRIPTION
Device Information ()	
System Name ()	This field displays the MAX-207HW2R system name. It is used for identification.
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**.
Hardware Version	This field displays the version of the physical device hardware.
Uptime	This field displays how long the MAX-207HW2R has been running since it last started up. The MAX-207HW2R starts up when you plug it in, when you restart it (**ADVANCED > System Configuration > Restart**), or when you reset it.
Memory Usage	This field displays what percentage of the MAX-207HW2R's memory is currently used. The higher the memory usage, the more likely the MAX-207HW2R is to slow down. Some memory is required just to start the MAX-207HW2R 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.
Interface Status	
LAN Interface	
Status	This field indicates whether or not the MAX-207HW2R is using the LAN interface. This field displays **Connected** when the MAX-207HW2R is using the LAN interface. Otherwise, it displays **DISCONNECTED**.
Rate	This field displays the LAN connection speed (in Mbps).
IP Address	This field displays the current IP address of the MAX-207HW2R in the LAN.
IP Mask	This field displays the current subnet mask on the LAN.
WAN Interface	
Status	This field indicates whether or not the MAX-207HW2R is using the WAN interface. This field displays **OPERATIONAL** when the MAX-207HW2R is using the WAN interface. Otherwise, it displays **DISCONNECTED**.
IP Address	This field displays the current IP address of the MAX-207HW2R in the LAN.
IP Mask	This field displays the current subnet mask in the LAN.
BSID	This field displays the identification number of the wireless base station to which the MAX-207HW2R is connected. Every base station transmits a unique BSID, which identifies it across the network.

Table 65 Status (continued)

LABEL	DESCRIPTION
Preamble Index	The Preamble Index is the number of bytes used for initial synchorinzation at the biginning of a downlink frame. See the IEEE 802.16e standard for more information.
Frequency	This field displays the radio frequency of the MAX-207HW2R's wireless connection to a base station.
Tx Bytes	This field shows the number of data packets uploaded from the MAX-207HW2R to the base station each second.
Rx Bytes	This field shows the number of data packets downloaded to the MAX-207HW2R from the base station each second.
RSSI	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. A strong signal does not necessarily indicate a good signal: a strong signal may have a low signal-to-noise ratio (SNR).
Tx Power	This field shows the output transmission (Tx) level of the MAX-207HW2R.
CINR	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.
MAC address	This field displays the Media Access Control address of the MAX-207HW2R. Every network device has a unique MAC address which identifies it across the network.

19

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
- MAX-207HW2R Access and Login
- Internet Access
- Phone Calls and VoIP
- Reset the MAX-207HW2R to Its Factory Defaults

19.1 Power, Hardware Connections, and LEDs

The MAX-207HW2R does not turn on. None of the LEDs turn on.

1 Make sure you are using the power adapter or cord included with the MAX-207HW2R.

2 Make sure the power adapter or cord is connected to the MAX-207HW2R 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 MAX-207HW2R.

4 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 1.2.1 on page 21 for more information.

2 Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adapter to the MAX-207HW2R.

5 If the problem continues, contact the vendor.

19.2 MAX-207HW2R Access and Login

I forgot the IP address for the MAX-207HW2R.

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 MAX-207HW2R 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 MAX-207HW2R (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 MAX-207HW2R to its factory defaults. See Section 19.1 on page 165.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the MAX-207HW2R to its factory defaults. See Section 9.4 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 3.2 on page 32), 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 MAX-207HW2R.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.2.1 on page 21.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix C on page 215.

4 If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. Your MAX-207HW2R 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 MAX-207HW2R. See Appendix D on page 225.

5 Reset the MAX-207HW2R to its factory defaults, and try to access the MAX-207HW2R with the default IP address. See Section 9.5 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 MAX-207HW2R using another service, such as Telnet. If you can access the MAX-207HW2R, check the remote management settings and firewall rules to find out why the MAX-207HW2R 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 MAX-207HW2R.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the MAX-207HW2R. Log out of the MAX-207HW2R 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 MAX-207HW2R.

4 If this does not work, you have to reset the MAX-207HW2R to its factory defaults. See Section 9.4 on page 93.

I cannot Telnet to the MAX-207HW2R.

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

19.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.2.1 on page 21.

2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 Check your security settings. 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 MAX-207HW2R 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 MAX-207HW2R, 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 MAX-207HW2R), but my Internet connection is not available any more.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.2.1 on page 21.

2 Disconnect and re-connect the power adapter to the MAX-207HW2R.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 The quality of the MAX-207HW2R’s wireless connection to the base station may be poor. Poor signal reception may be improved by moving the MAX-207HW2R 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 MAX-207HW2R away or switch the other devices off. Weather conditions may also affect signal quality.

3 As well as having an external antenna connector, the MAX-210HW2 is equipped with an internal directional antenna. If you know the location of the base station, orient the front of the MAX-207HW2R (the side with the LEDs) towards the base station. If you do not know the location of the base station, experiment by moving the MAX-207HW2R while observing the **Strength Indicator** LEDs for an increase in received signal strength. The MAX-200HW2 and MAX-230HW2 do not have internal antennas.

4 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.2.1 on page 21. If the MAX-207HW2R is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

5 Disconnect and re-connect the power adapter to the MAX-207HW2R.

6 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.

19.4 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

1 Check the telephone connections and telephone wire.

2 Make sure you have the **VOICE > Service Configuration > SIP Settings** screen properly configured (Chapter 10 on page 97).

I can access the Internet, but cannot make VoIP calls.

1 Make sure you have the **VOICE > Service Configuration > SIP Settings** screen properly configured (Chapter 10 on page 97).

2 The **VoIP** LED should come on. Make sure that your telephone is connected to the **VoIP** port (see the Quick Start Guide for information on connecting telephone cables to the these ports).

3 You can also check the VoIP status in the **Status** screen.

4 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you cannot make a call using speed dial, there may be something wrong with the SIP server. Contact your VoIP service provider.

Problems With Multiple SIP Accounts

You can set up two SIP accounts on your MAX-207HW2R. By default your MAX-207HW2R uses SIP account 1 for outgoing calls, and it uses SIP accounts 1 and 2 for incoming calls. With this setting, you always use SIP account 1 for your outgoing calls and you cannot distinguish which SIP account the calls are coming in through. If you want to control the use of different dialing plans for accounting purposes or other reasons, you need to configure your phone port in order to control which SIP account you are using when placing or receiving calls.

19.5 Reset the MAX-207HW2R to Its Factory Defaults

If you reset the MAX-207HW2R, you lose all of the changes you have made. The MAX-207HW2R re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

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

To reset the MAX-207HW2R,

1 Make sure the **Power** LED is on and not blinking.

2 Press and hold the **Reset** button for five to ten seconds. Release the **Reset** button when the **Power** LED begins to blink. The default settings have been restored.

If the MAX-207HW2R restarts automatically, wait for the MAX-207HW2R to finish restarting, and log in to the web configurator. The password is “284wj/6”.

If the MAX-207HW2R does not restart automatically, disconnect and reconnect the MAX-207HW2R’s power. Then, follow the directions above again.

19.5.1 Pop-up Windows, JavaScripts and Java Permissions

Please see Appendix C on page 215.

20

Product Specifications

This chapter gives details about your MAX-207HW2R's hardware and firmware features.

Table 66 Environmental and Hardware Specifications

FEATURE	DESCRIPTION
Operating Temperature	0°C to 45°C
Storage Temperature	-25°C to 55°C
Operating Humidity	10% ~ 90% (non-condensing)
Storage Humidity	10% to 95% (non-condensing)
Power Supply	12V DC, 2A
Power consumption	18W
Ethernet Interface	Four auto-negotiating, auto-MDI/MDI-X NWay 10/100 Mbps RJ-45 Ethernet ports
Telephony Interface	Two analog ATA interfaces for standard telephones through RJ-11 FXS (Foreign Exchange Subscriber) analog connector
Antennas	Two internal omnidirectional 5dBi WiMAX antennas
Weight	400 g
Dimensions	165 mm (W) x 25 mm (D) x 260 mm (H)
Certification	Safety: UL 60950-1 EMI and EMS: FCC & WiMAX Forum Wave II compliance

Table 67 Radio Specifications

FEATURE	DESCRIPTION
Media Access Protocol	IEEE 802.16e
WiMAX Bandwidth	2.5 GHz

Table 67 Radio Specifications (continued)

Data Rate	Download: Maximum 20 Mbps Average 6 Mbps Upload: Maximum 4 Mbps Average 3 Mbps
Modulation	QPSK (uplink and downlink) 16-QAM (uplink and downlink) 64-QAM (downlink only)
Output Power	Typically 26 dBm with internal antennas
Duplex mode	Time Division Duplex (TDD)
Security	PKMv2 EAP CCMP, 128-bit AES

Table 68 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 MAX-207HW2R. You must connect using a compatible web browser in order to use it.
High Speed Wireless Internet Access	The MAX-207HW2R 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 MAX-207HW2R is a WiMAX mobile station (MS) compatible with the IEEE 802.16e standard.
Firewall	The MAX-207HW2R 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 MAX-207HW2R’s firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	The MAX-207HW2R 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).

Table 68 Firmware Specifications (continued)

FEATURE	DESCRIPTION
Universal Plug and Play (UPnP)	Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.
Dynamic DNS Support	With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.
DHCP	DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Your device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
Multiple SIP Accounts	You can configure multiple voice (SIP) accounts.
SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic (up to 60 ms). This helps ensure good voice quality for your conversations.
Voice Activity Detection/ Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Echo Cancellation	You device supports G.168 of at least 24 ms. This an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Time and Date	Get the current time and date from an external server when you turn on your MAX-207HW2R. You can also set the time manually.
Logging	Use the MAX-207HW2R’s logging feature to view connection history, surveillance logs, and error messages.
Codecs	Enhanced Variable Rate Codec (EVRC), G.711 (PCM µ-law and a-law), G.729a, and G.723.1

Table 68 Firmware Specifications (continued)

FEATURE	DESCRIPTION
Fax Support	T.38 FAX relay (FAX over UDP). G.711 fax relay for fax calls and be able to renegotiate codec to G.711 if a fax call is detected.
Ring Tones	Supports different distinctive ring tones on each line.
Call Prioritization	Prioritize VoIP traffic originating from the RJ-11 ports over any other traffic.

Table 69 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 2833	Real-time Transport Protocol Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2976	The SIP INFO Method
RFC 3261	Session Initiation Protocol (SIP version 2)
RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP).
RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3323	A Privacy Mechanism for SIP
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

Table 69 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 3550	RTP - A Real Time Protocol for Real-Time Applications
RFC 3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)-XR
RFC 3715	IP Sec/NAT Compatibility
RFC 3842	A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
IEEE 802.3	10BASE5 10 Mbit/s (1.25 MB/s)
IEEE 802.3u	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) with auto-negotiation

Table 70 Voice Features

Call Park and Pickup	Call park and pickup lets you put a call on hold (park) and then continue the call (pickup). The caller must still pay while the call is parked. When you park the call, you enter a number of your choice (up to eight digits), which you must enter again when you pick up the call. If you do not enter the correct number, you cannot pickup the call. This means that only someone who knows the number you have chosen can pick up the call. You can have more than one call on hold at the same time, but you must give each call a different number.
Call Return	With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.
Country Code	Phone standards and settings differ from one country to another, so the settings on your MAX-207HW2R must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the MAX-207HW2R from one country to another.
Do not Disturb (DnD)	This feature allows you to set your phone not to ring when someone calls you. You can set each phone independently using its keypad, or configure global settings for all phones using the command line interpreter.
Auto Dial	You can set the MAX-207HW2R to automatically dial a specified number immediately whenever you lift a phone off the hook. Use the Web Configurator to set the specified number. Use the command line interpreter to have the MAX-207HW2R wait a specified length of time before dialing the number.
Phone config	The phone configuration table allows you to customize the phone keypad combinations you use to access certain features on the MAX-207HW2R, such as call waiting, call return, call forward, etc. The phone configuration table is configurable in command interpreter mode.

Table 70 Voice Features

Firmware update enable / disable	If your service provider uses this feature, you hear a recorded message when you pick up the phone when new firmware is available for your MAX-207HW2R. Enter *99# in your phone's keypad to have the MAX-207HW2R upgrade the firmware, or enter #99# to not upgrade. If your service provider gave you different numbers to use, enter them instead. If you enter the code to not upgrade, you can make a call as normal. You will hear the recording again each time you pick up the phone, until you upgrade.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.
Call forwarding	With this feature, you can set the MAX-207HW2R to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
Caller ID	The MAX-207HW2R supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.
SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Other Voice Features	SIP version 2 (Session Initiating Protocol RFC 3261) SDP (Session Description Protocol RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Voice codecs (coder/decoders) G.711, G.726, G.729 Fax and data modem discrimination DTMF Detection and Generation DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO) Point-to-point call establishment between two IADs Quick dialing through predefined phone book, which maps the phone dialing number and destination URL. Flexible Dial Plan (RFC3525 section 7.1.14)

Table 71 Star (*) and Pound (#) Code Support

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

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

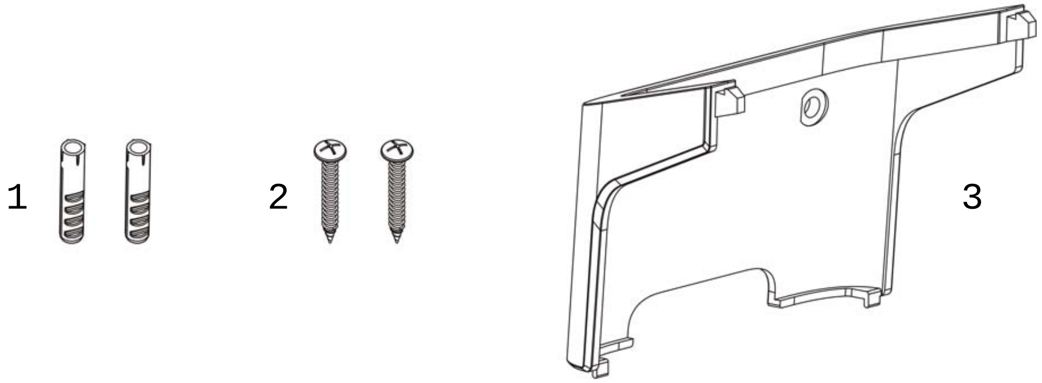
Not all features are supported by all service providers. Consult your service provider for more information.

20.1 Wall-Mounting

This section shows you how to mount your MAX-207HW2R on a wall using the ZyXEL Wall-Mounting kit (not included).

20.1.1 The Wall-Mounting Kit

The wall-mounting kit contains the following parts:



1 Two Mortar Plugs (M4*L30 mm)

2 Two Screws (M4*L30 mm)

3 Wall-Mounting Chassis

If any parts are missing, contact your vendor.

20.1.2 Instructions

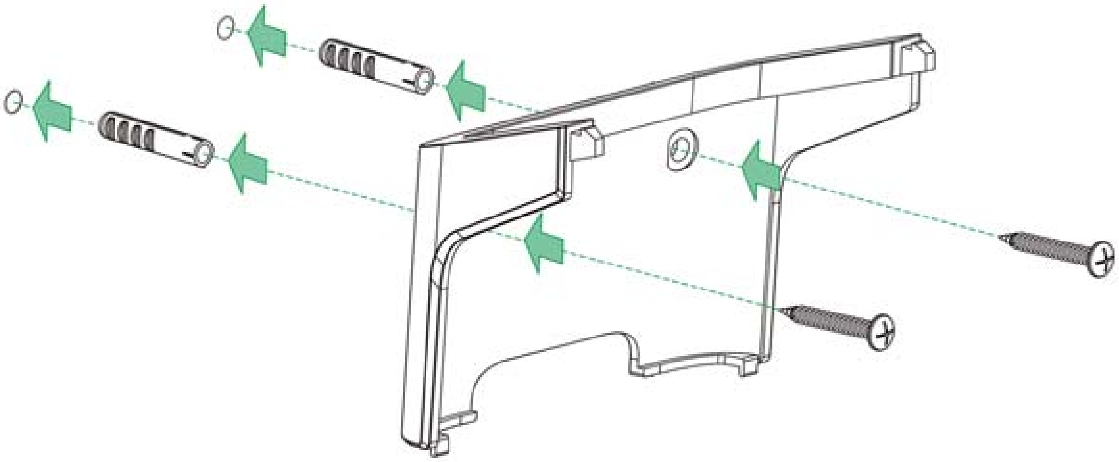
To mount the MAX-207HW2R on a wall:

1 Select a position free of obstructions on a sturdy wall.

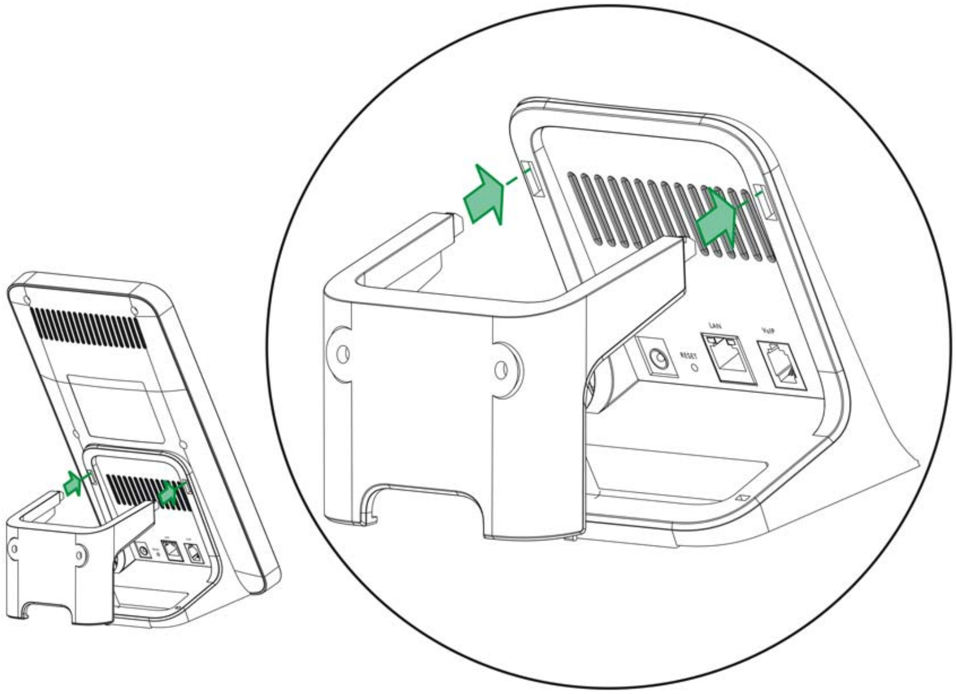
2 Drill two holes in the wall exactly 70 mm apart. The holes should be 6 mm wide and at least 30 mm deep.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 Attach the wall mounting chassis with the plugs and screws as shown below:

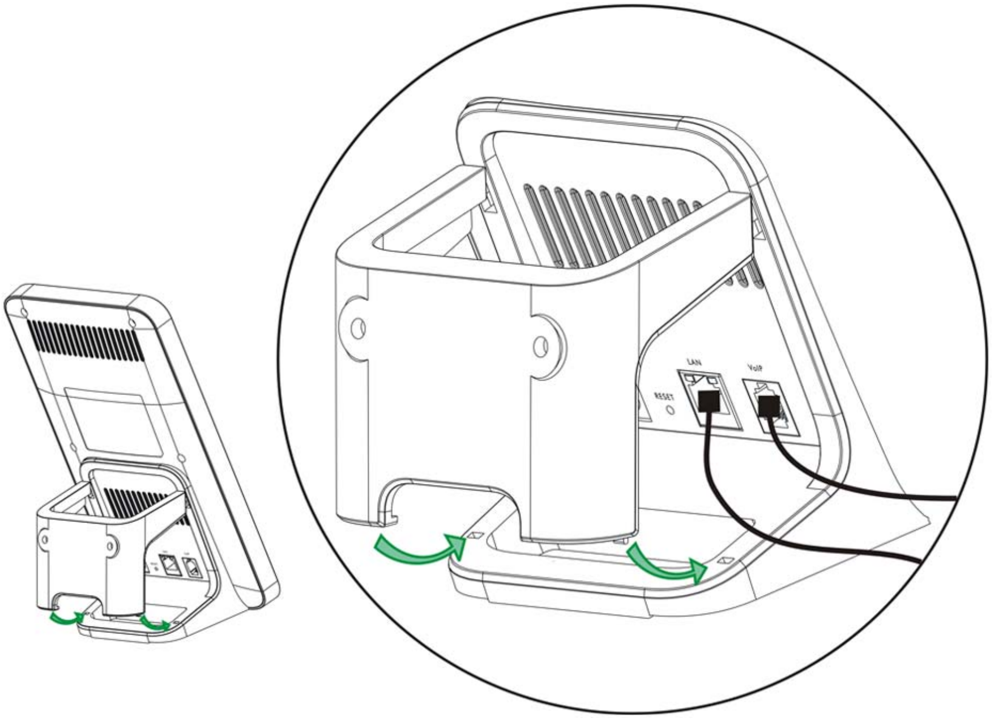


4 Connect the MAX-207HW2R to the wall mounting chassis by snapping the chassis' two upper chassis hooks into the matching holes on the MAX-207HW2R:

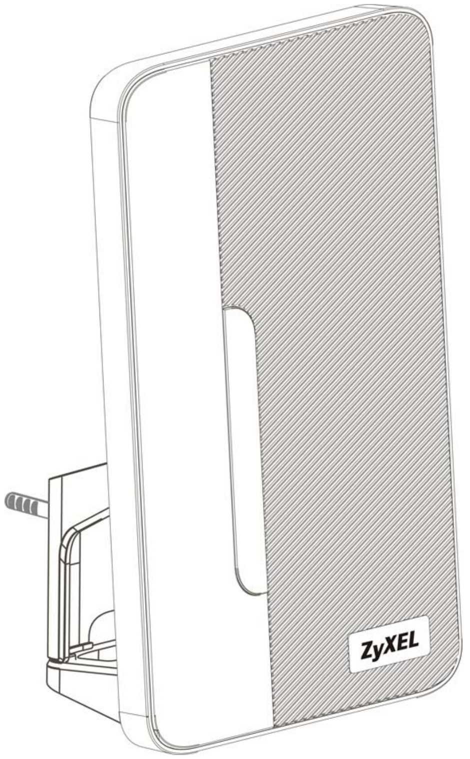


Do not pinch or server the cable connections between the wall-mounting chassis the MAX-207HW2R.

5 Snap the lower chassis hooks into the matching holes on the MAX-207HW2R. The cable connections should come out either the left or right gaps between the wall-mounting chassis and the MAX-207HW2R



6 Once you have snapped the wall-mounting chassis in place, the MAX-207HW2R is securely fastened to the wall.



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 MAX-207HW2R 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.

Setting Up Your Computer's IP Address

Note: Your specific ZyXEL device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

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:

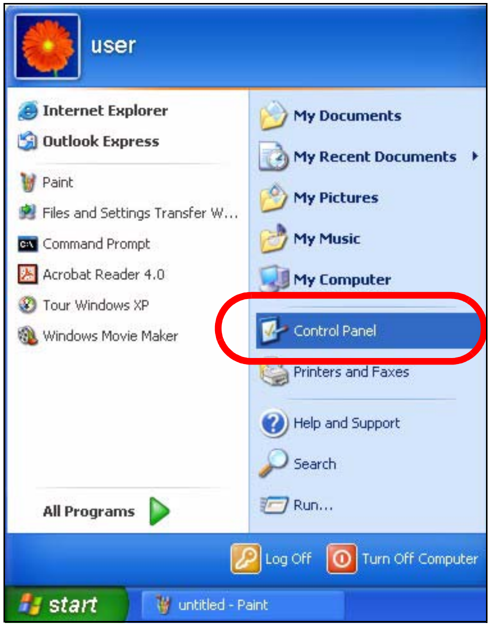
- Windows XP/NT/2000 on page 188
- Windows Vista on page 191
- Mac OS X: 10.3 and 10.4 on page 195
- Mac OS X: 10.5 on page 199
- Linux: Ubuntu 8 (GNOME) on page 202
- Linux: openSUSE 10.3 (KDE) on page 208

Windows XP/NT/2000

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

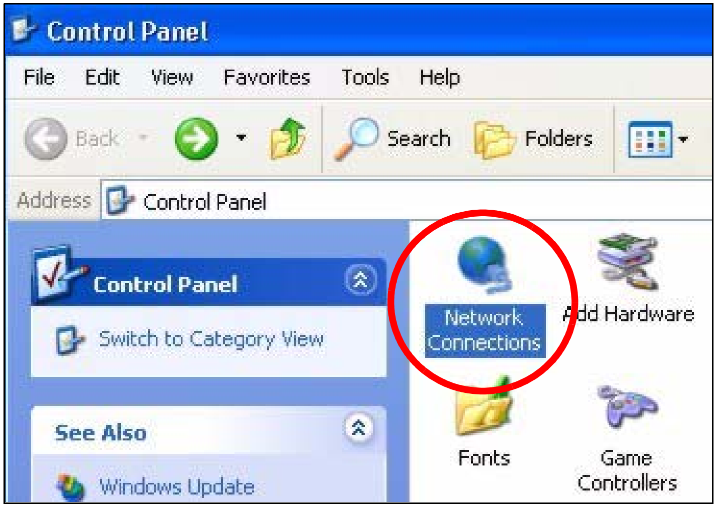
1 Click **Start** > **Control Panel**.

Figure 74 Windows XP: Start Menu



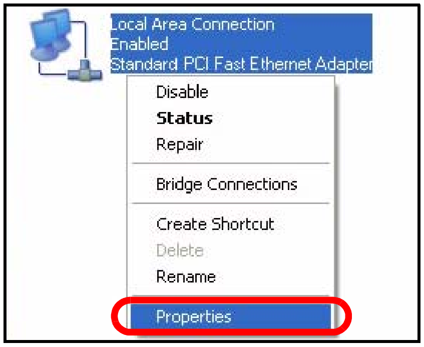
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 75 Windows XP: Control Panel



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

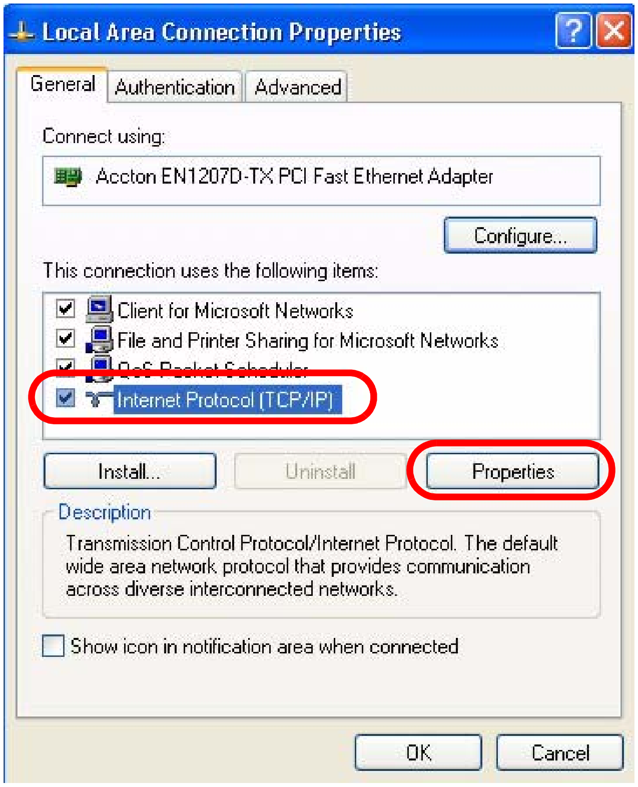
Figure 76 Windows XP: Control Panel > Network Connections > Properties



Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter

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

Figure 77 Windows XP: Local Area Connection Properties



Local Area Connection Properties

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

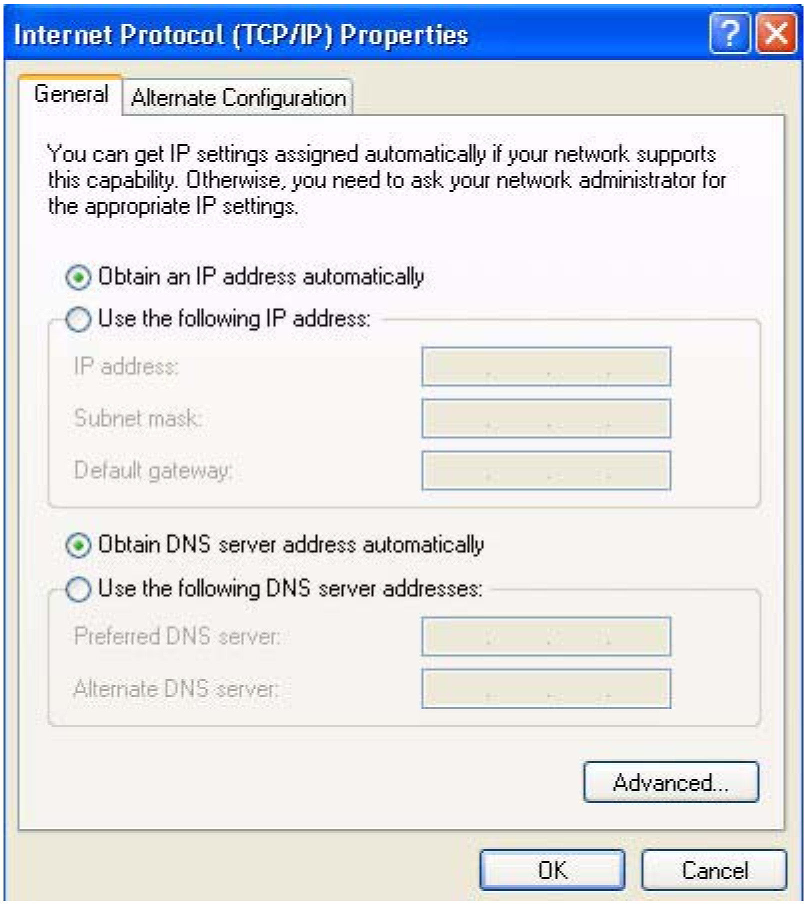
Description

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

□ Show icon in notification area when connected

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

Figure 78 Windows XP: Internet Protocol (TCP/IP) Properties



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

● Obtain an IP address automatically

○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

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].

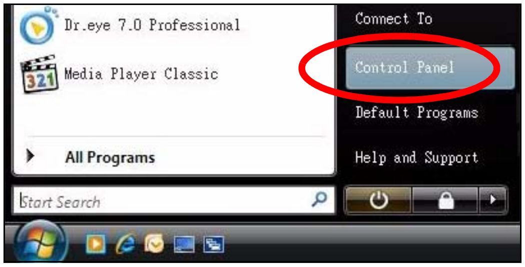
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

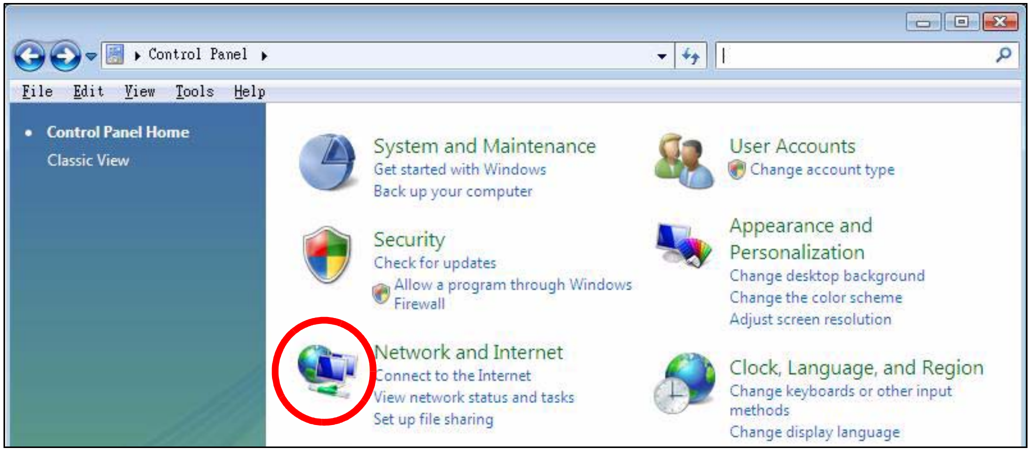
1 Click **Start** > **Control Panel**.

Figure 79 Windows Vista: Start Menu



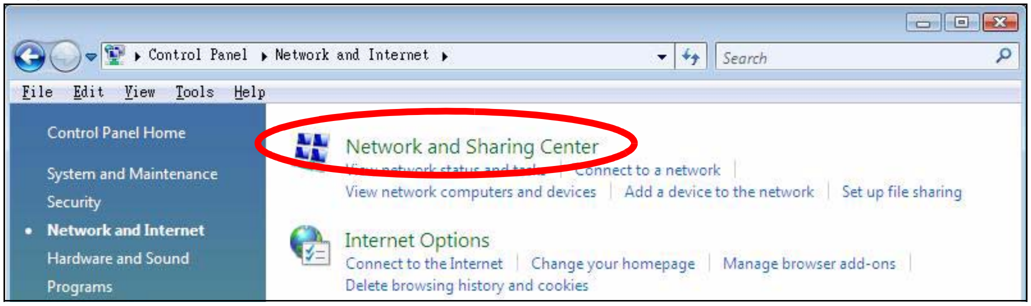
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 80 Windows Vista: Control Panel



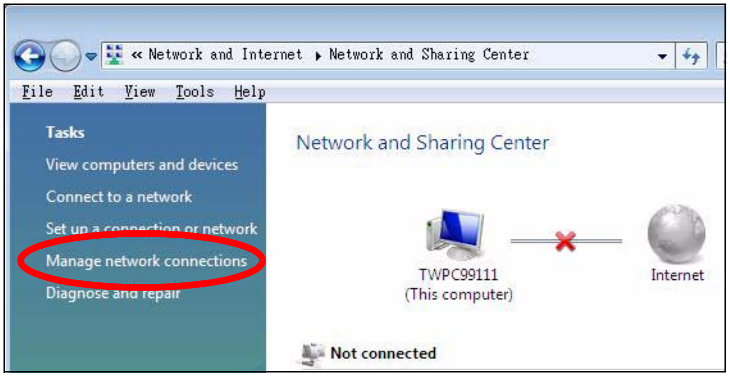
3 Click the **Network and Sharing Center** icon.

Figure 81 Windows Vista: Network And Internet



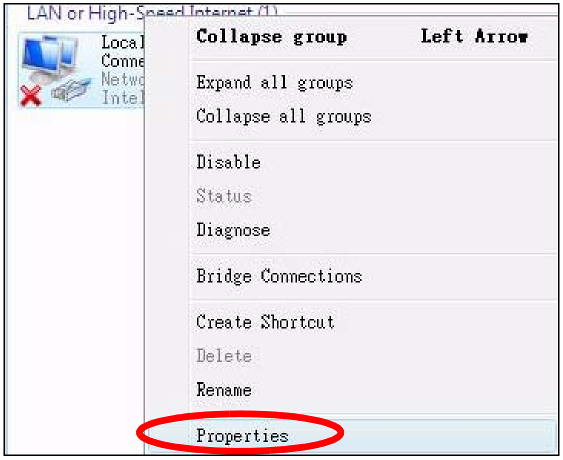
4 Click **Manage network connections**.

Figure 82 Windows Vista: Network and Sharing Center


« Network and Internet ▸ Network and Sharing Center
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
TWPC99111
(This computer)
Internet
Not connected

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

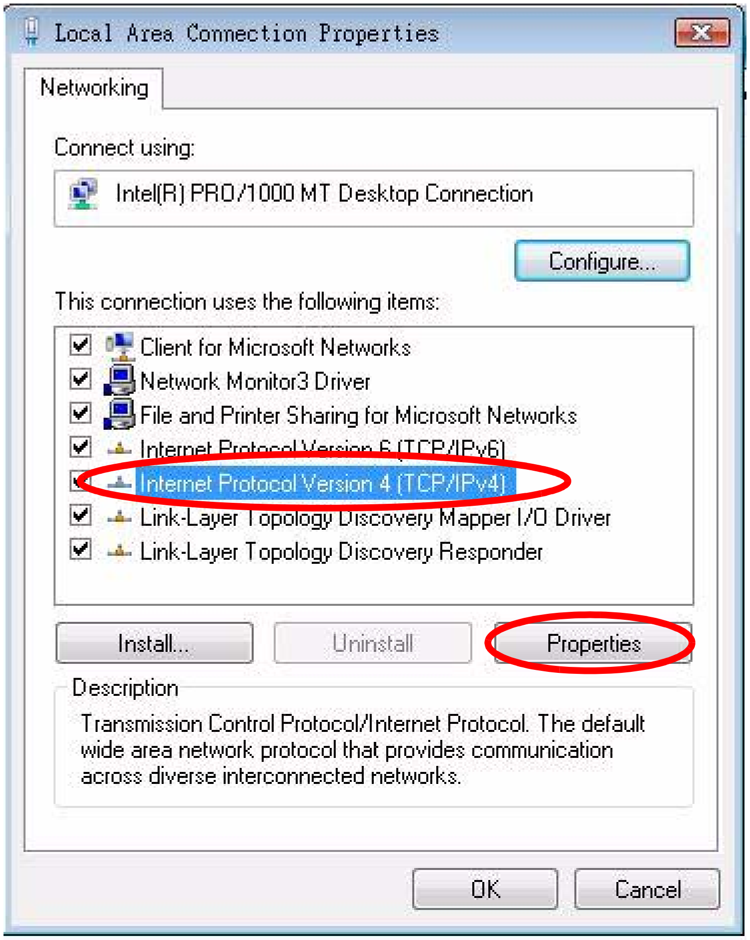
Figure 83 Windows Vista: Network and Sharing Center



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 84 Windows Vista: Local Area Connection Properties



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Connection

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Network Monitor3 Driver
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

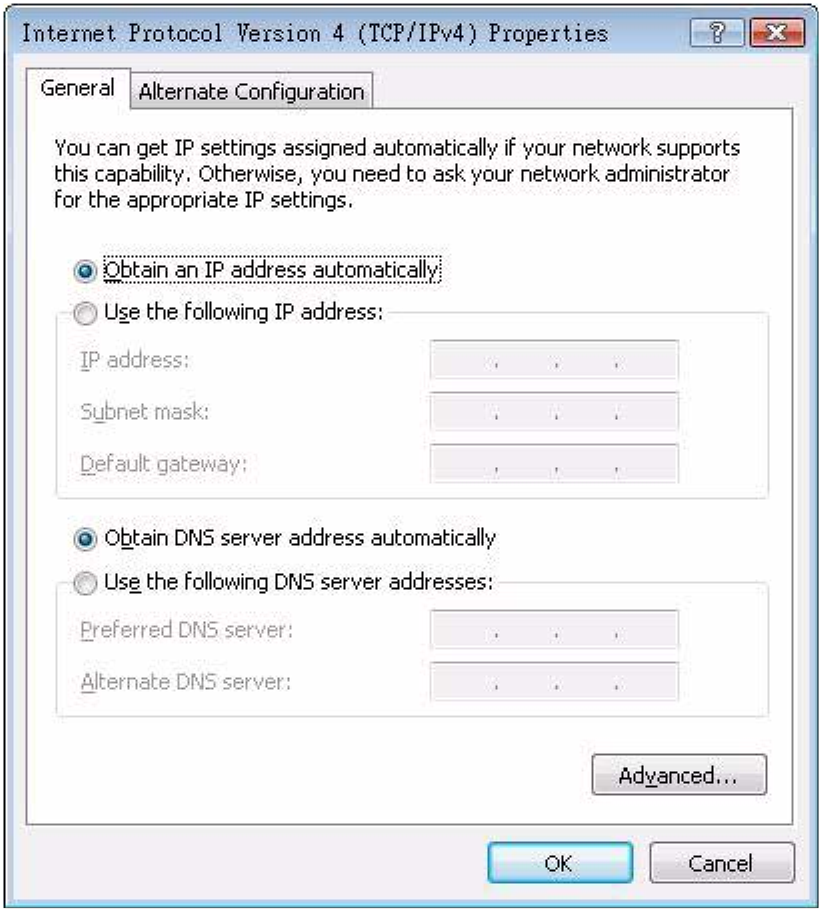
Description

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

OK Cancel

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

Figure 85 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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].

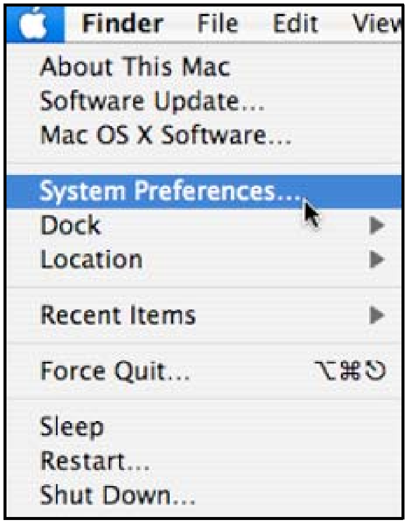
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

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.

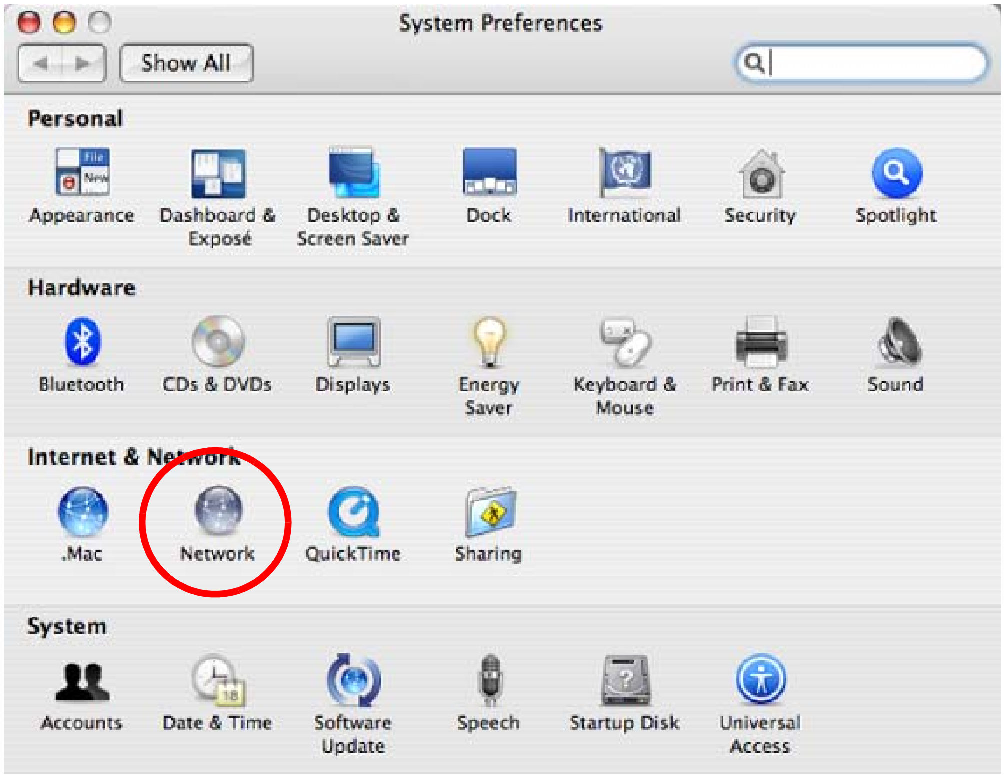
1 Click **Apple** > **System Preferences**.

Figure 86 Mac OS X 10.4: Apple Menu



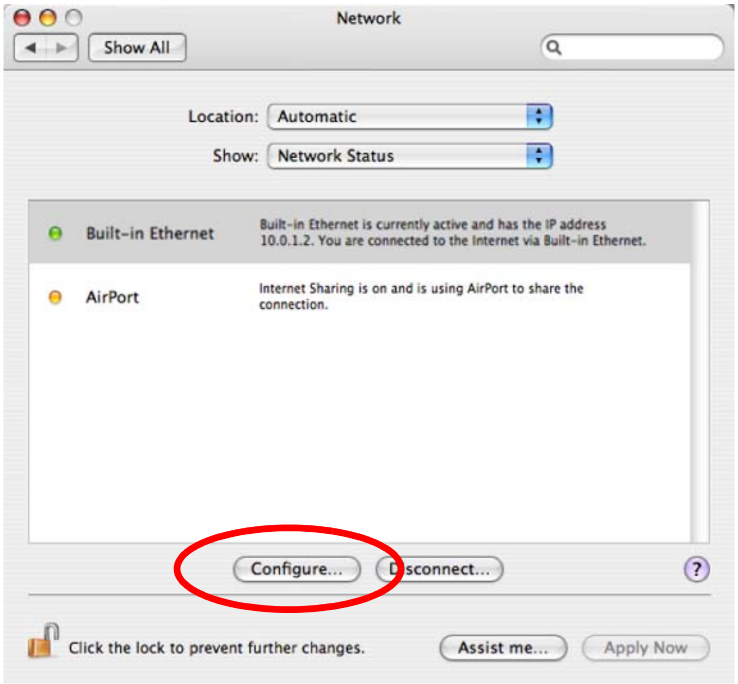
2 In the **System Preferences** window, click the **Network** icon.

Figure 87 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 88 Mac OS X 10.4: Network Preferences



Location: Automatic

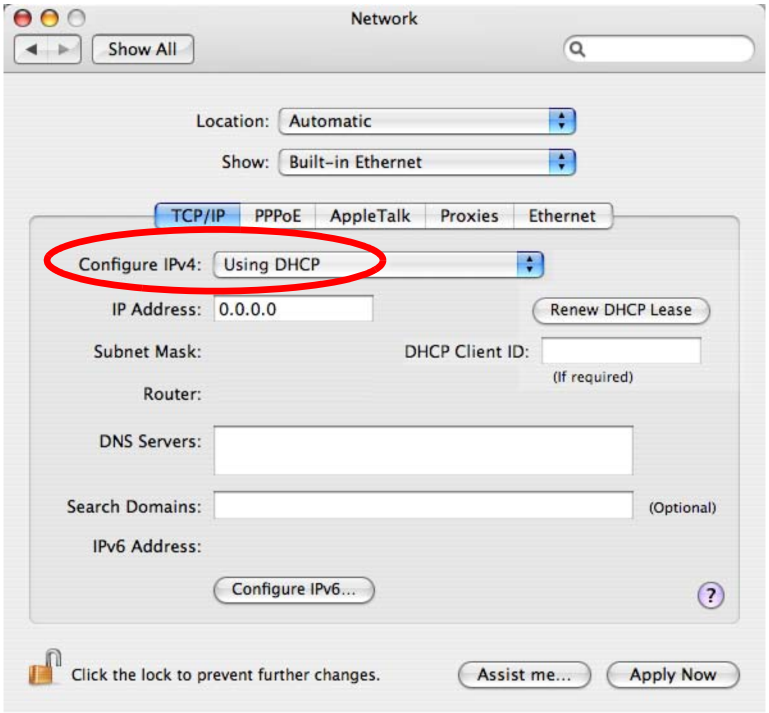
Show: Network Status

Built-in Ethernet — Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.

AirPort — Internet Sharing is on and is using AirPort to share the connection.

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

Figure 89 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 0.0.0.0

Subnet Mask:

DHCP Client ID: (If required)

Router:

DNS Servers:

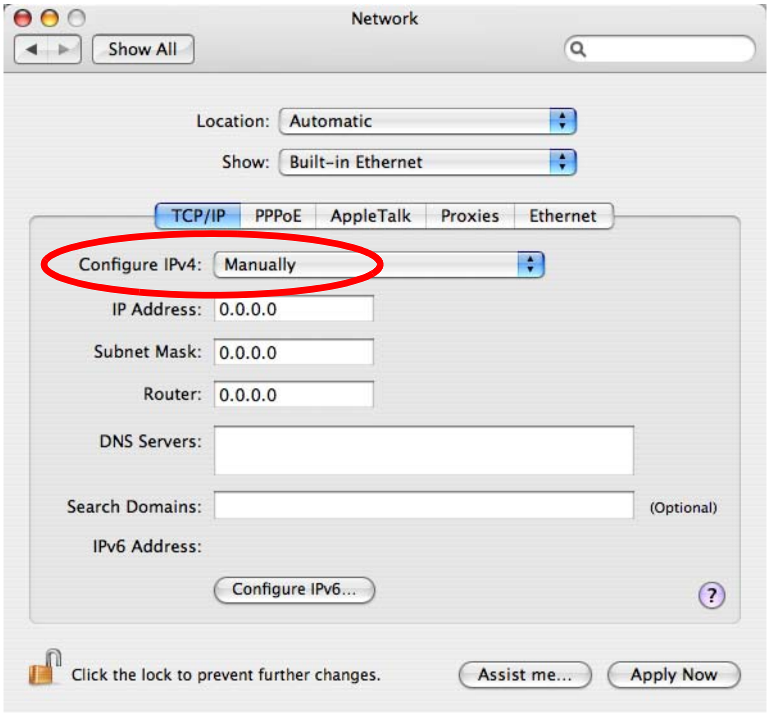
Search Domains: (Optional)

IPv6 Address:

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 90 Mac OS X 10.4: Network Preferences > Ethernet



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Manually

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Router: 0.0.0.0

DNS Servers:

Search Domains: (Optional)

IPv6 Address:

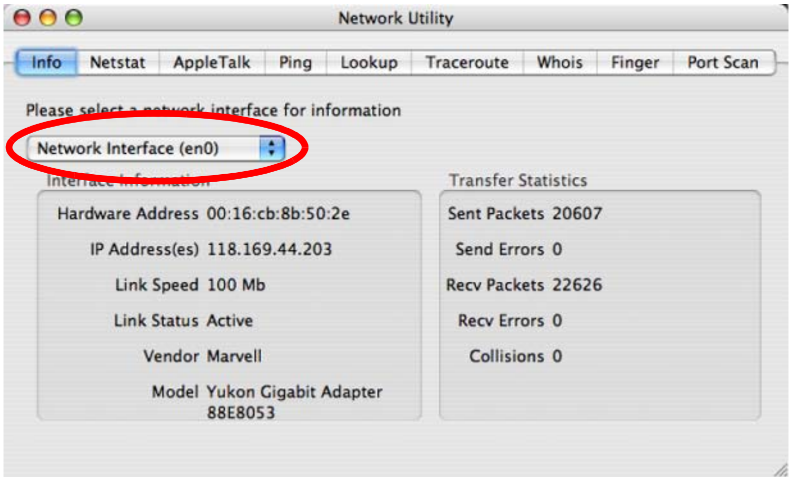
Click the lock to prevent further changes.

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 91 Mac OS X 10.4: Network Utility



Please select a network interface for information

Network Interface (en0)

Interface Information

Hardware Address 00:16:cb:8b:50:2e

IP Address(es) 118.169.44.203

Link Speed 100 Mb

Link Status Active

Vendor Marvell

Model Yukon Gigabit Adapter 88E8053

Transfer Statistics

Sent Packets 20607

Send Errors 0

Recv Packets 22626

Recv Errors 0

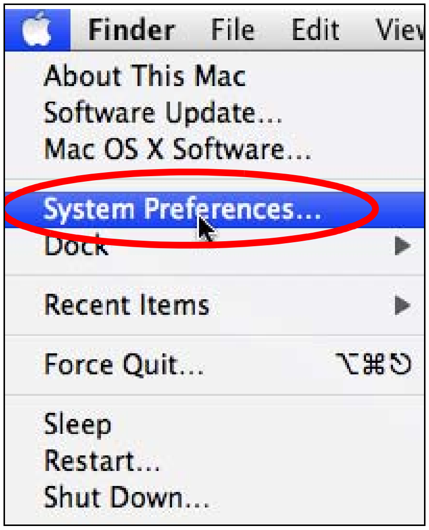
Collisions 0

Mac OS X: 10.5

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

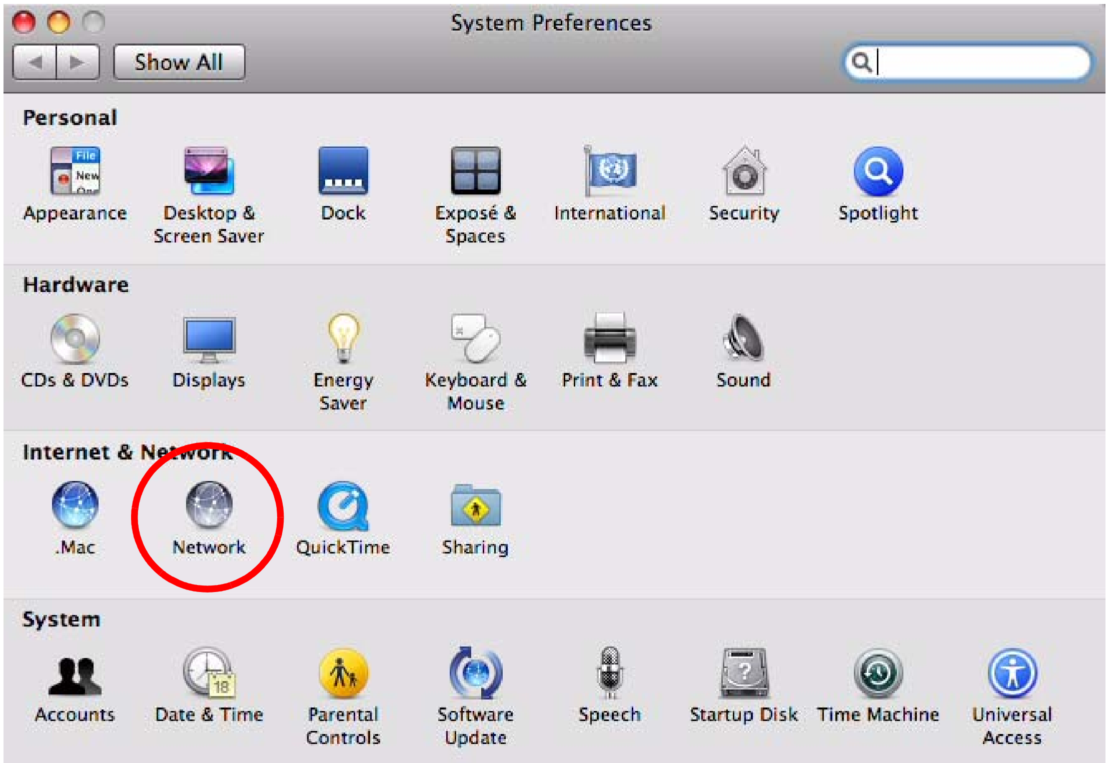
1 Click **Apple** > **System Preferences**.

Figure 92 Mac OS X 10.5: Apple Menu



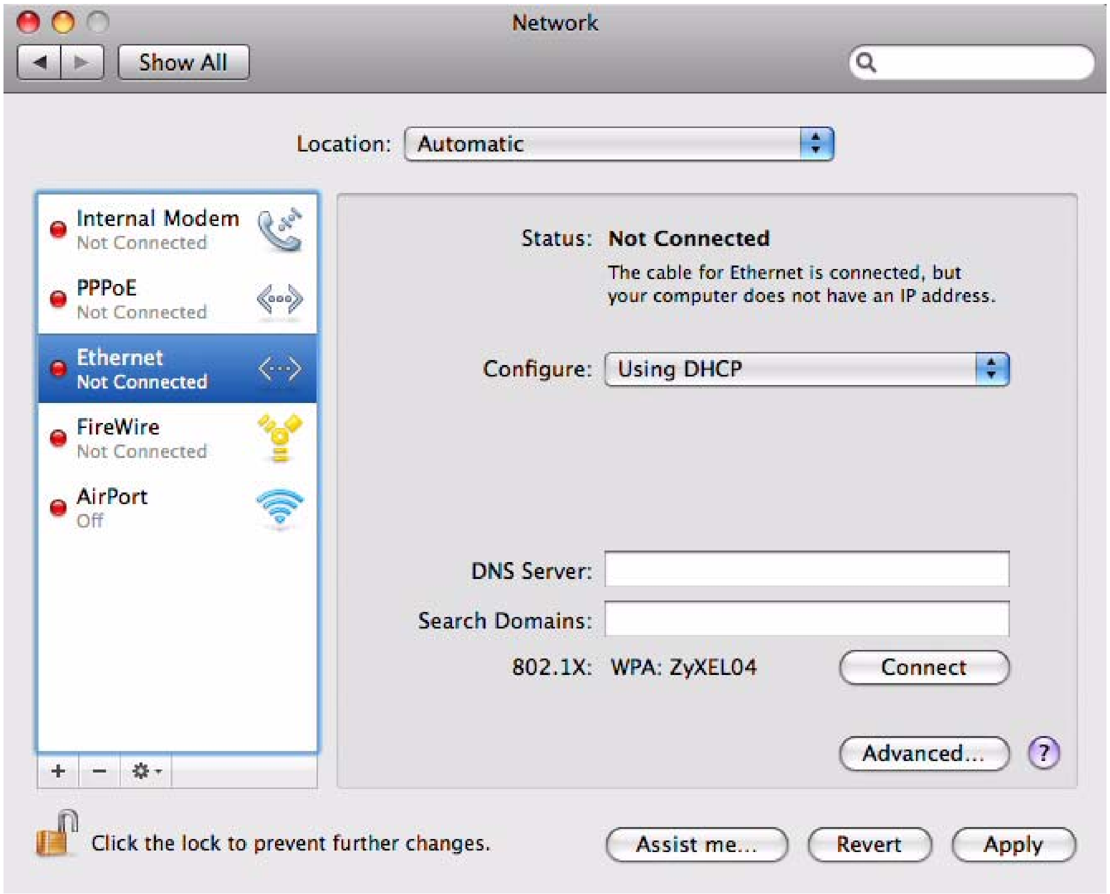
2 In **System Preferences**, click the **Network** icon.

Figure 93 Mac OS X 10.5: Systems Preferences



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

Figure 94 Mac OS X 10.5: Network Preferences > Ethernet



Location: Automatic

Status: **Not Connected**

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Using DHCP

DNS Server:

Search Domains:

802.1X: WPA: ZyXEL04

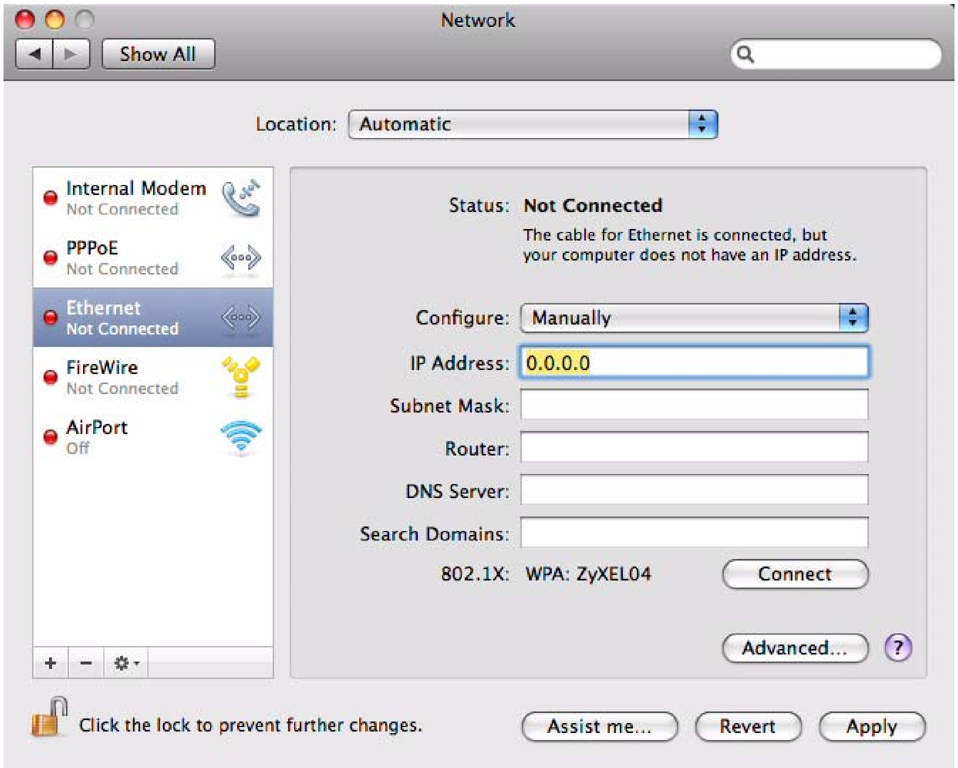
4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

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 MAX-207HW2R.

Figure 95 Mac OS X 10.5: Network Preferences > Ethernet



Location: Automatic

Internal Modem
Not Connected

PPPoE
Not Connected

Ethernet
Not Connected

FireWire
Not Connected

AirPort
Off

Status: **Not Connected**

The cable for Ethernet is connected, but
your computer does not have an IP address.

Configure: Manually

IP Address: 0.0.0.0

Subnet Mask:

Router:

DNS Server:

Search Domains:

802.1X: WPA: ZyXEL04

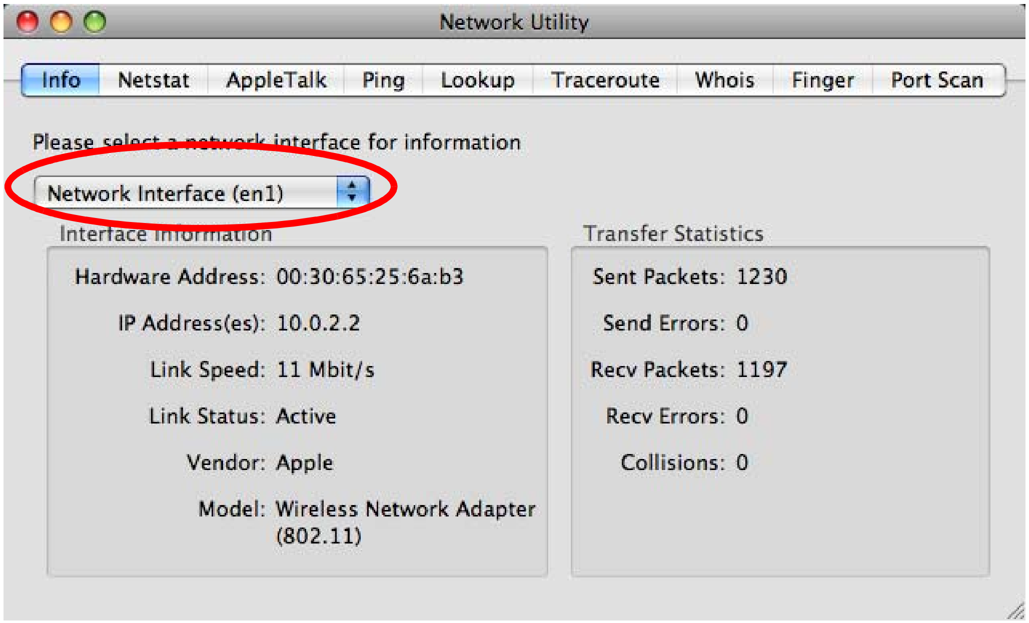
Click the lock to prevent further changes.

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 96 Mac OS X 10.5: Network Utility



Please select a network interface for information

Network Interface (en1)

Interface Information

Hardware Address: 00:30:65:25:6a:b3
IP Address(es): 10.0.2.2
Link Speed: 11 Mbit/s
Link Status: Active
Vendor: Apple
Model: Wireless Network Adapter (802.11)

Transfer Statistics

Sent Packets: 1230
Send Errors: 0
Recv Packets: 1197
Recv Errors: 0
Collisions: 0

Linux: Ubuntu 8 (GNOME)

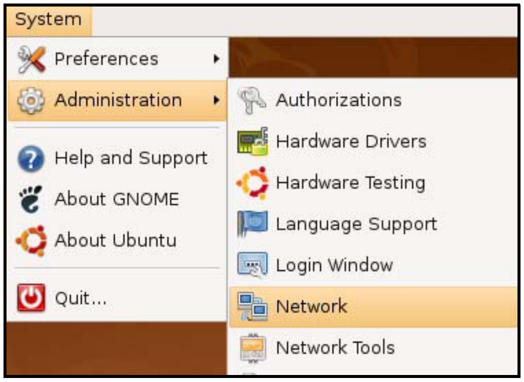
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

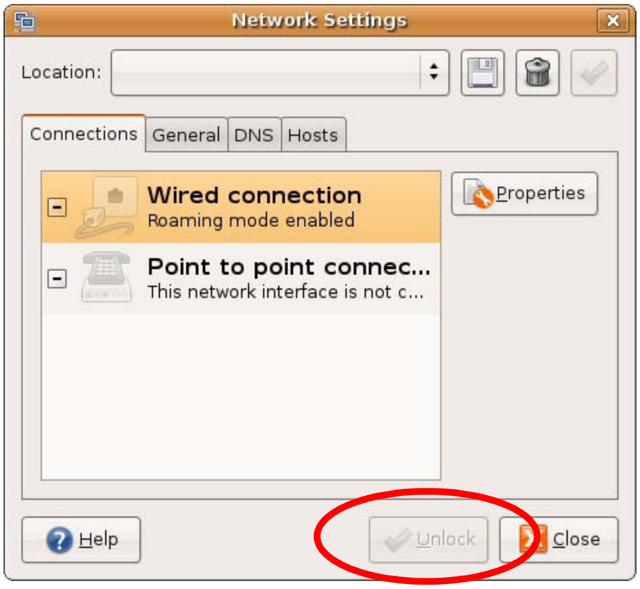
1 Click **System > Administration > Network**.

Figure 97 Ubuntu 8: System > Administration Menu



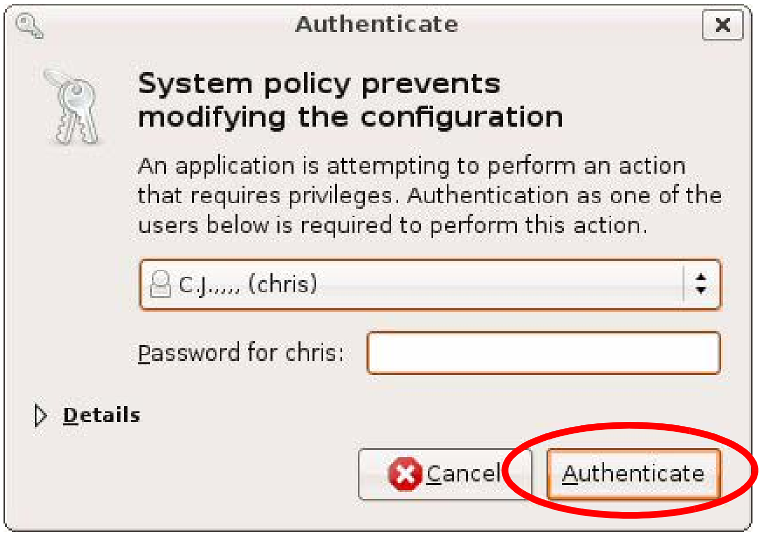
2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 98 Ubuntu 8: Network Settings > Connections



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

Figure 99 Ubuntu 8: Administrator Account Authentication



Authenticate

System policy prevents modifying the configuration

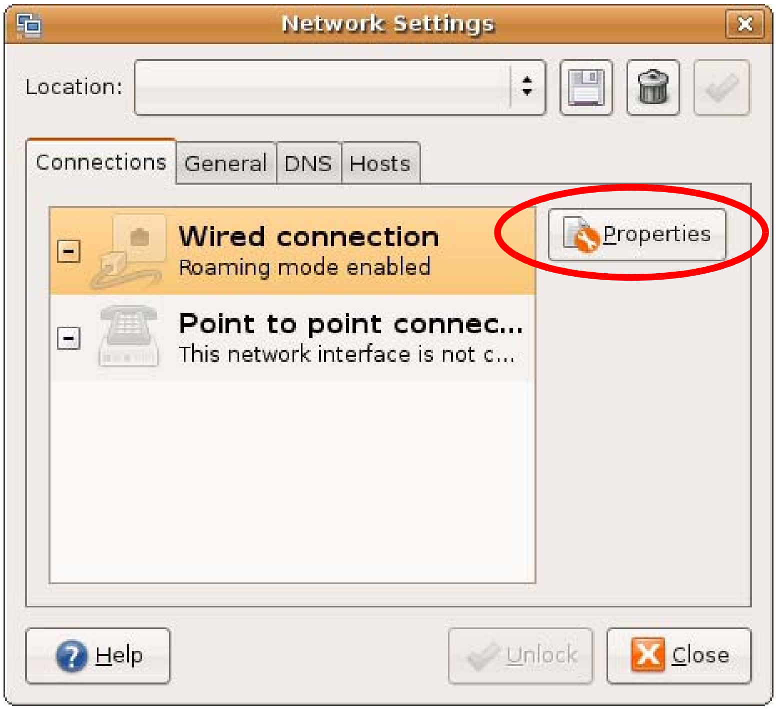
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.

C.J..,,, (chris)

Password for chris:

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

Figure 100 Ubuntu 8: Network Settings > Connections

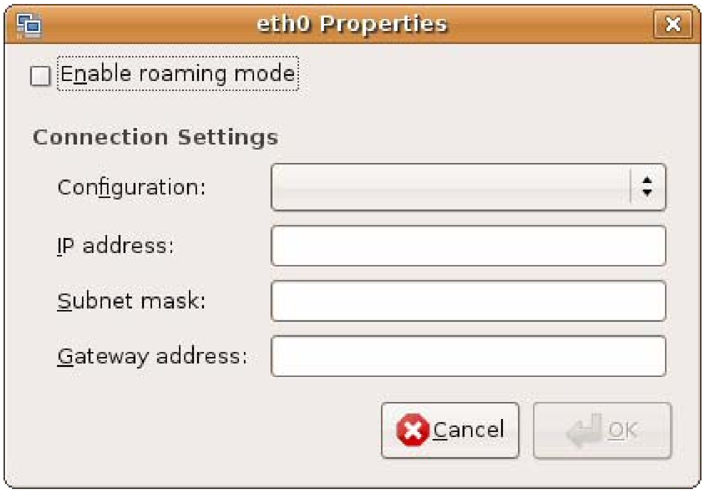


Wired connection
Roaming mode enabled

Point to point connec...
This network interface is not c...

5 The **Properties** dialog box opens.

Figure 101 Ubuntu 8: Network Settings > Properties

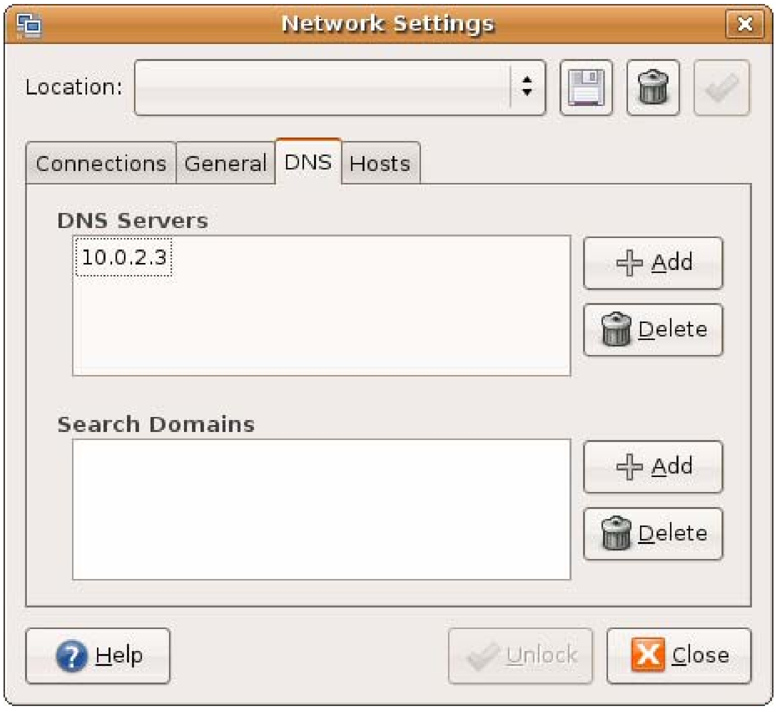


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

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 102 Ubuntu 8: Network Settings > DNS



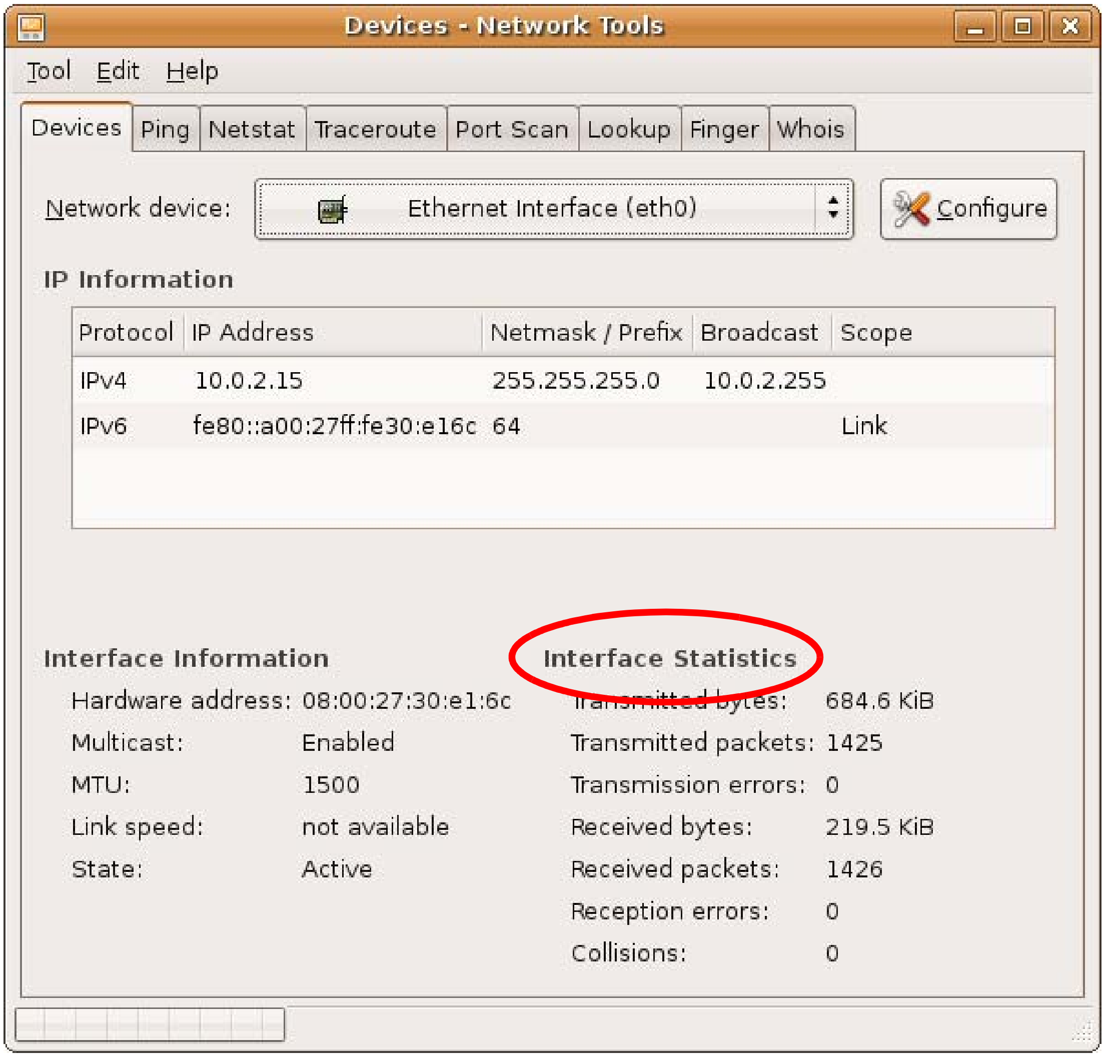
10.0.2.3

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 103 Ubuntu 8: Network Tools



Network device: Ethernet Interface (eth0)

IP Information

Protocol	IP Address	Netmask / Prefix	Broadcast	Scope
IPv4	10.0.2.15	255.255.255.0	10.0.2.255	
IPv6	fe80::a00:27ff:fe30:e16c	64		Link

Interface Information

Hardware address:	08:00:27:30:e1:6c
Multicast:	Enabled
MTU:	1500
Link speed:	not available
State:	Active

Interface Statistics

Transmitted bytes:	684.6 KiB
Transmitted packets:	1425
Transmission errors:	0
Received bytes:	219.5 KiB
Received packets:	1426
Reception errors:	0
Collisions:	0

Linux: openSUSE 10.3 (KDE)

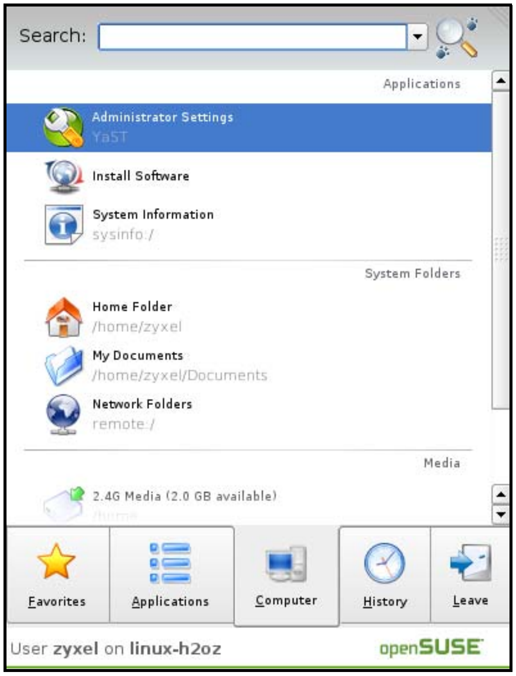
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

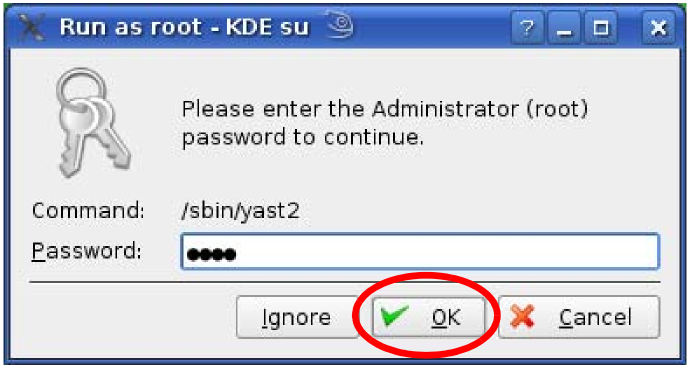
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 104 openSUSE 10.3: K Menu > Computer Menu



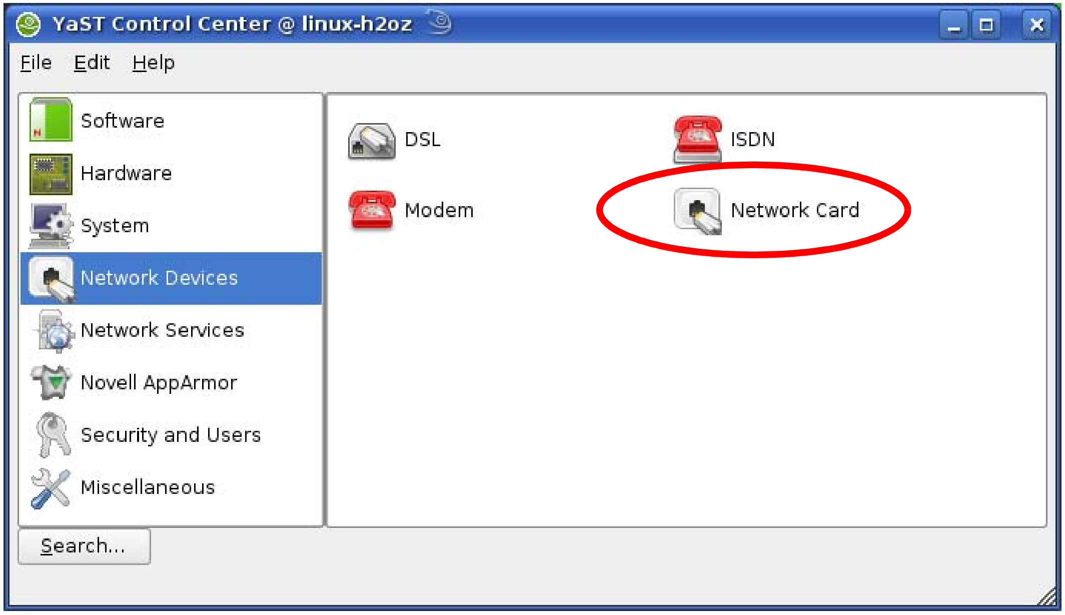
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 105 openSUSE 10.3: K Menu > Computer Menu



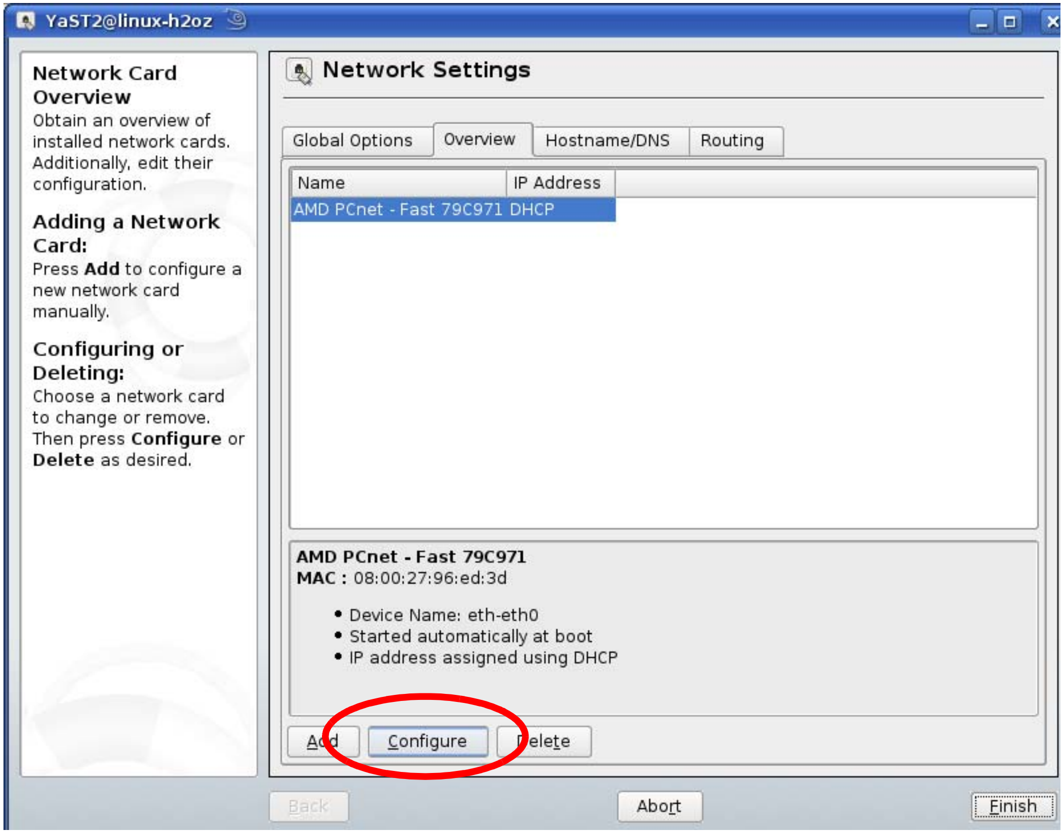
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 106 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 107 openSUSE 10.3: Network Settings



Network Card Overview
Obtain an overview of installed network cards. Additionally, edit their configuration.

Adding a Network Card:
Press **Add** to configure a new network card manually.

Configuring or Deleting:
Choose a network card to change or remove. Then press **Configure** or **Delete** as desired.

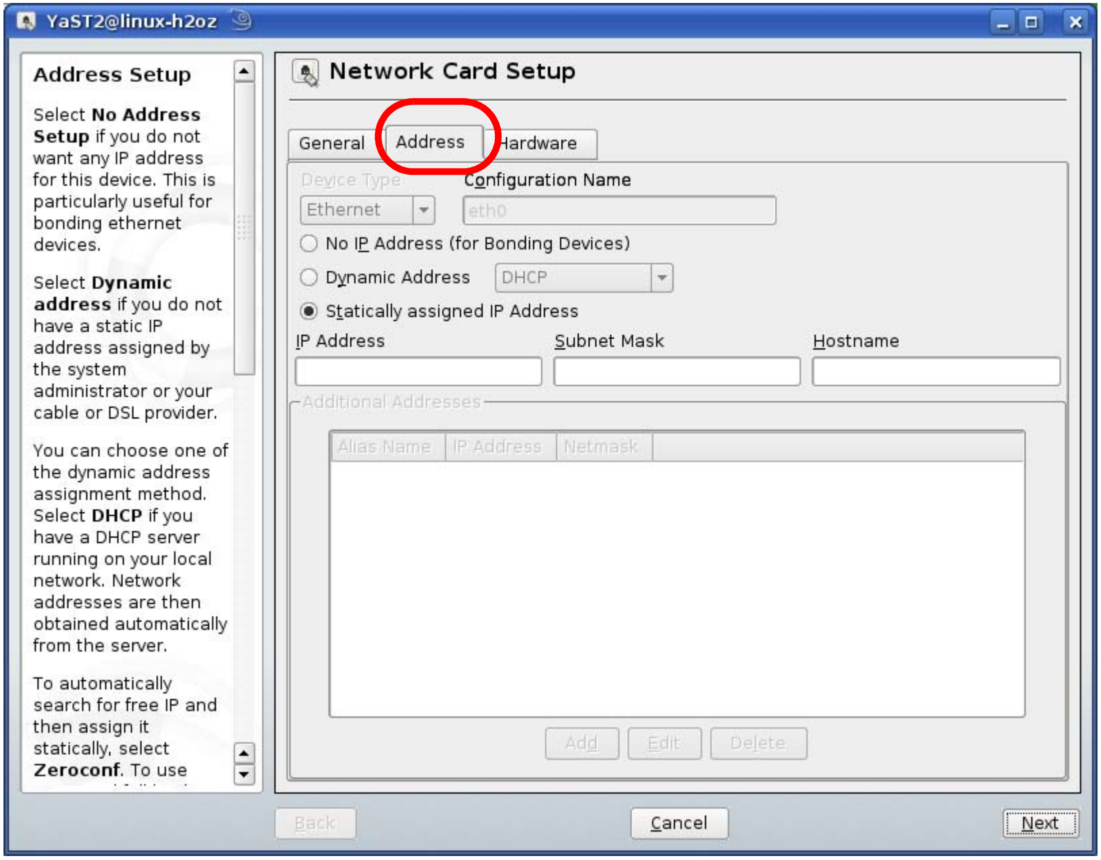
Name	IP Address
AMD PCnet - Fast 79C971	DHCP

AMD PCnet - Fast 79C971
MAC : 08:00:27:96:ed:3d

- Device Name: eth-eth0
- Started automatically at boot
- IP address assigned using DHCP

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

Figure 108 openSUSE 10.3: Network Card Setup



Address Setup

Select **No Address Setup** if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.

Select **Dynamic address** if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.

You can choose one of the dynamic address assignment method. Select **DHCP** if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.

To automatically search for free IP and then assign it statically, select **Zeroconf**. To use

Network Card Setup

Device Type: Ethernet

Configuration Name: eth0

○ No IP Address (for Bonding Devices)

○ Dynamic Address DHCP

● Statically assigned IP Address

IP Address | Subnet Mask | Hostname

Additional Addresses

Alias Name	IP Address	Netmask

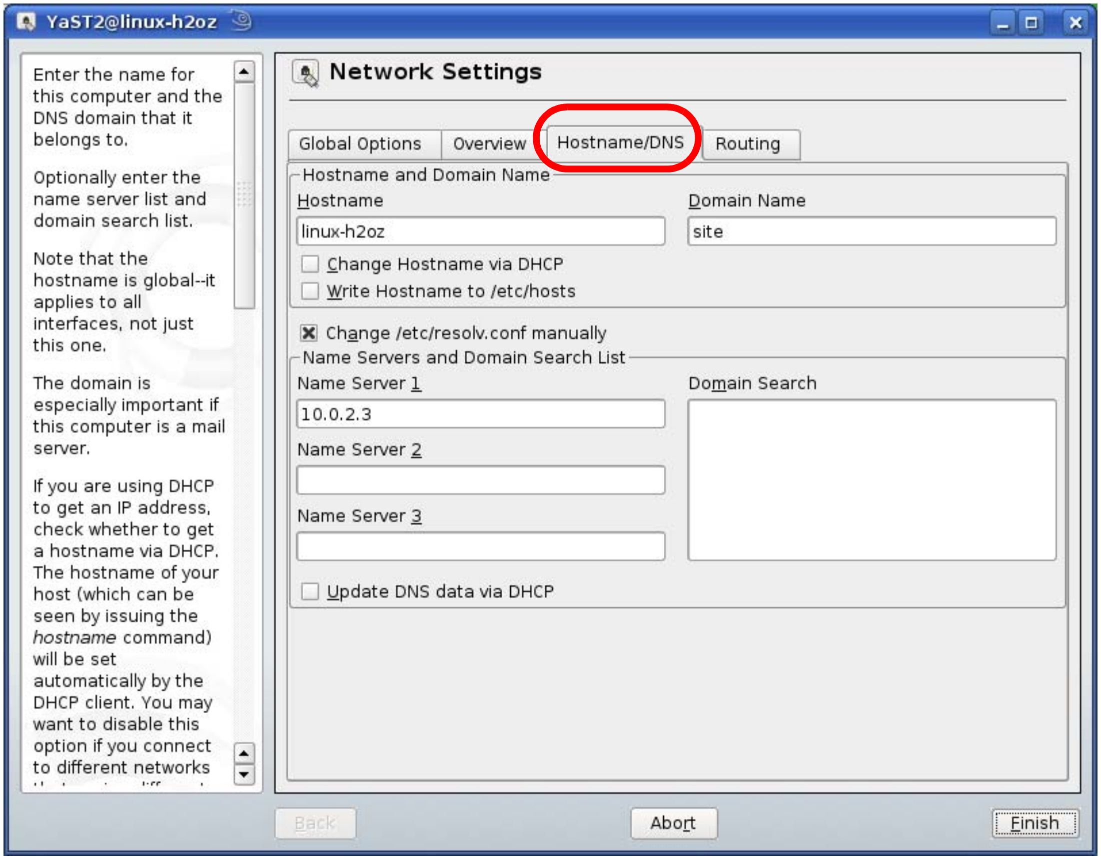
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

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 109 openSUSE 10.3: Network Settings



Enter the name for this computer and the DNS domain that it belongs to.

Optionally enter the name server list and domain search list.

Note that the hostname is global--it applies to all interfaces, not just this one.

The domain is especially important if this computer is a mail server.

If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the *hostname* command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks

Hostname and Domain Name

Hostname: linux-h2oz

Domain Name: site

☐ Change Hostname via DHCP

☐ Write Hostname to /etc/hosts

☒ Change /etc/resolv.conf manually

Name Servers and Domain Search List

Name Server 1: 10.0.2.3

Name Server 2:

Name Server 3:

Domain Search:

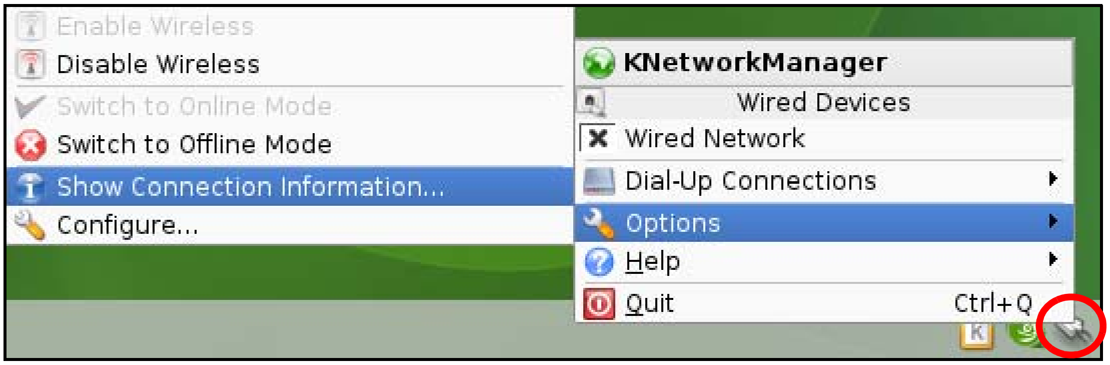
☐ Update DNS data via DHCP

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

Verifying Settings

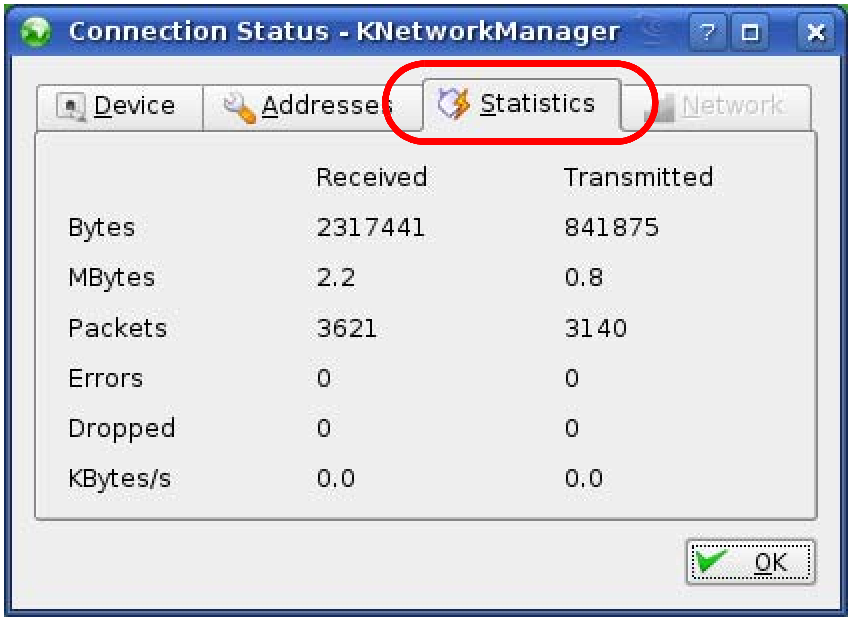
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 110 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 111 openSUSE: Connection Status - KNetwork Manager



	Received	Transmitted
Bytes	2317441	841875
MBytes	2.2	0.8
Packets	3621	3140
Errors	0	0
Dropped	0	0
KBytes/s	0.0	0.0

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: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

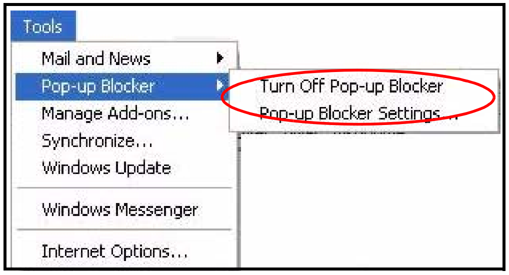
You may have to disable pop-up blocking to log into your device.

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 112 Pop-up Blocker

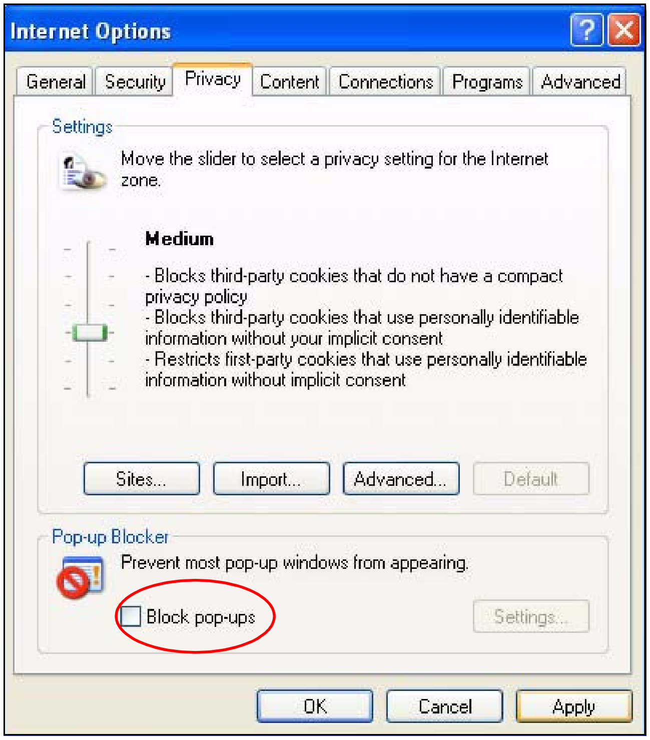


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 113 Internet Options: Privacy



Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Move the slider to select a privacy setting for the Internet zone.
Medium
- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent
Sites...
Import...
Advanced...
Default
Pop-up Blocker
Prevent most pop-up windows from appearing.
□ Block pop-ups
Settings...
OK
Cancel
Apply

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

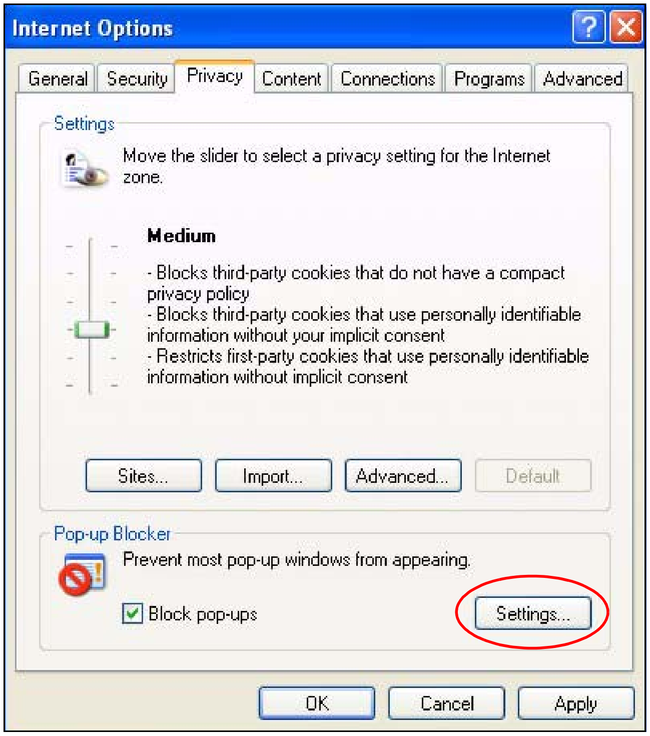
Enable Pop-up Blockers with Exceptions

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 114 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

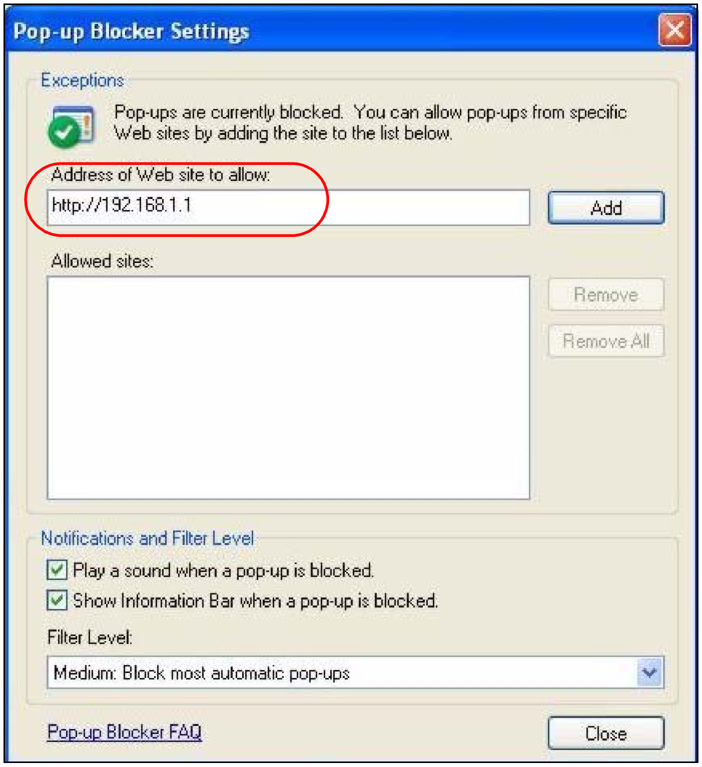
Prevent most pop-up windows from appearing.

☑ Block pop-ups

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 115 Pop-up Blocker Settings



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

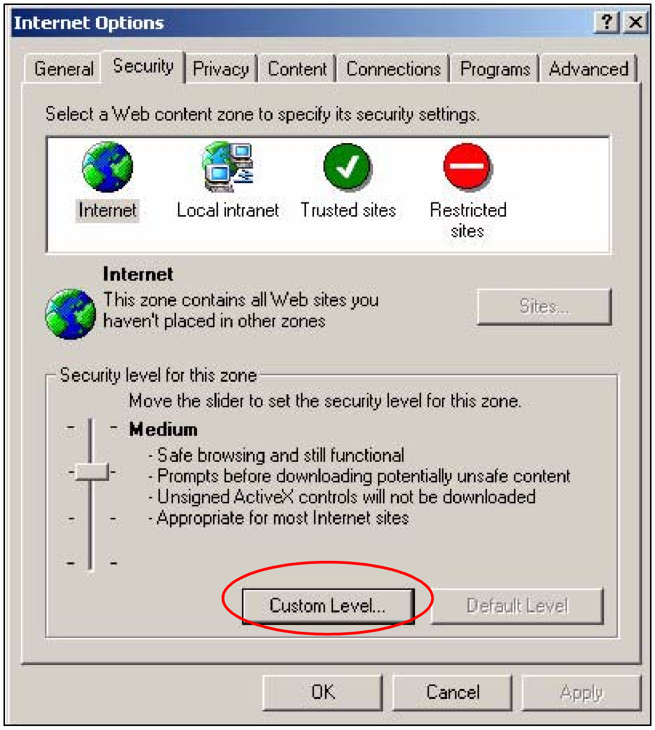
6 Click **Apply** to save this setting.

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 116 Internet Options: Security



Select a Web content zone to specify its security settings.

This zone contains all Web sites you haven't placed in other zones

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

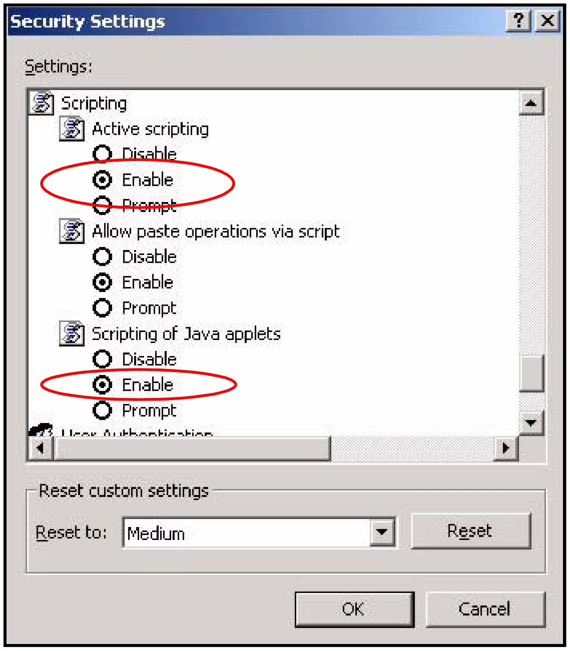
3 Scroll down to **Scripting**.

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 117 Security Settings - Java Scripting



Scripting

Active scripting
○ Disable
● Enable
○ Prompt

Allow paste operations via script
○ Disable
● Enable
○ Prompt

Scripting of Java applets
○ Disable
● Enable
○ Prompt

User Authentication

Reset to: Medium

Java Permissions

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

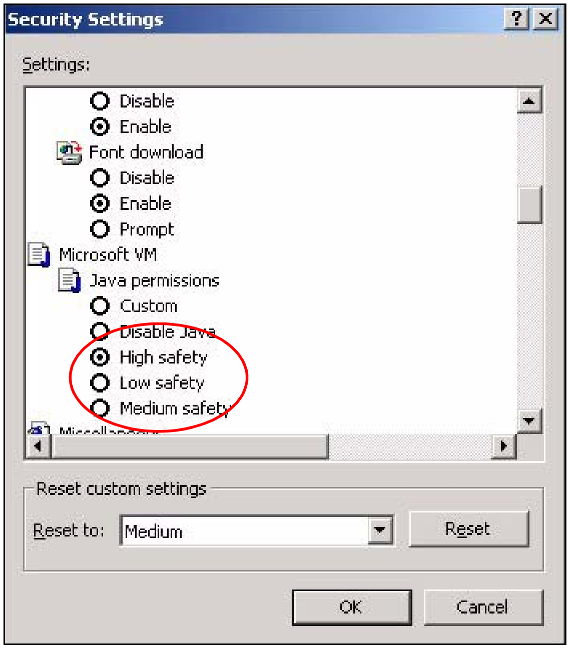
2 Click the **Custom Level...** button.

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 118 Security Settings - Java



Security Settings

Settings:

○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

Reset custom settings

Reset to: Medium

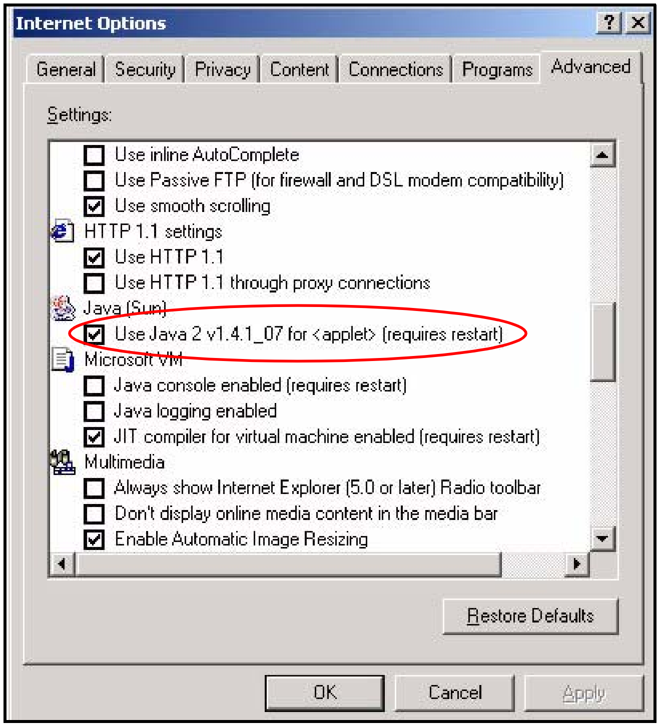
JAVA (Sun)

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 119 Java (Sun)



- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- □ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- □ Java console enabled (requires restart)
- □ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

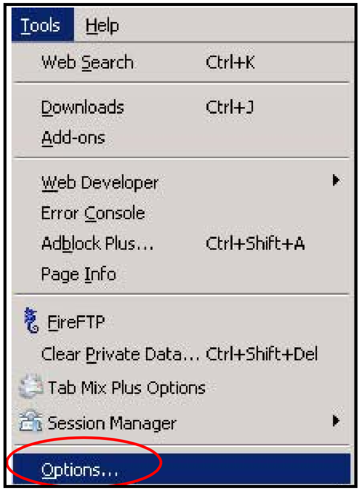
- □ Always show Internet Explorer (5.0 or later) Radio toolbar
- □ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

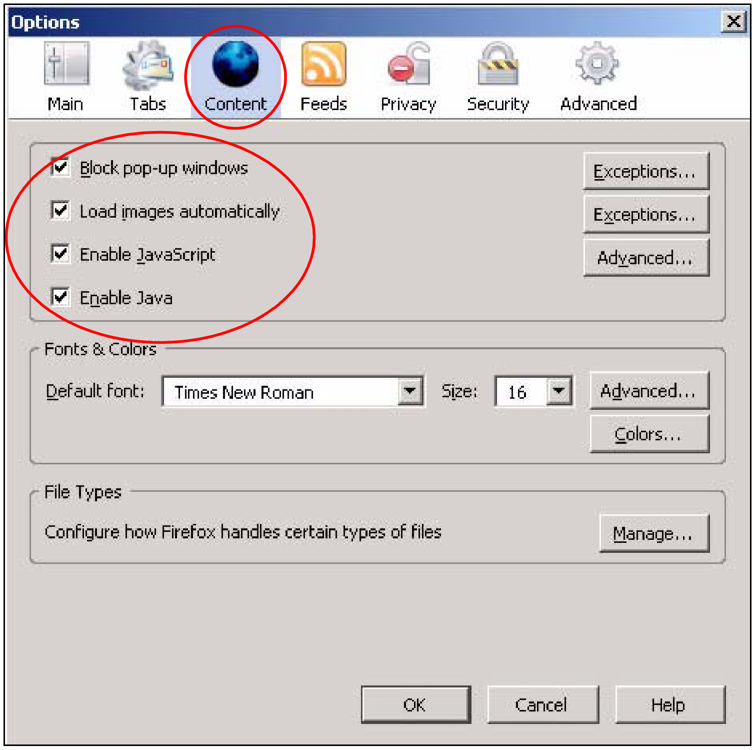
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 120 Mozilla Firefox: TOOLS > Options



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

Figure 121 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman

Size: 16

File Types

Configure how Firefox handles certain types of files

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.

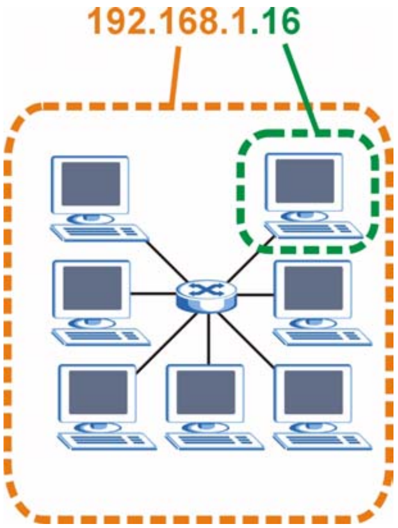
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.100.1). 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 122 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 72 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 73 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 74 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 75 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

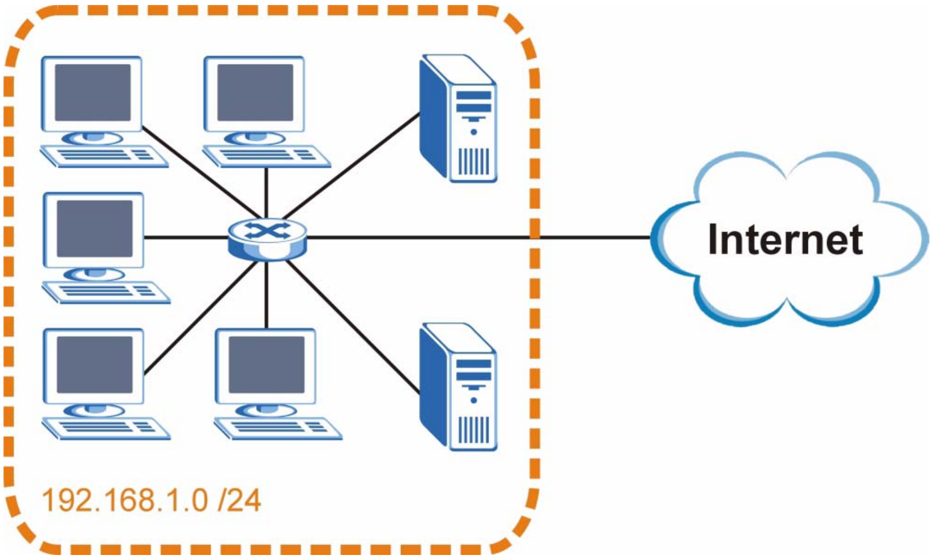
Subnetting

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 123 Subnetting Example: Before Subnetting

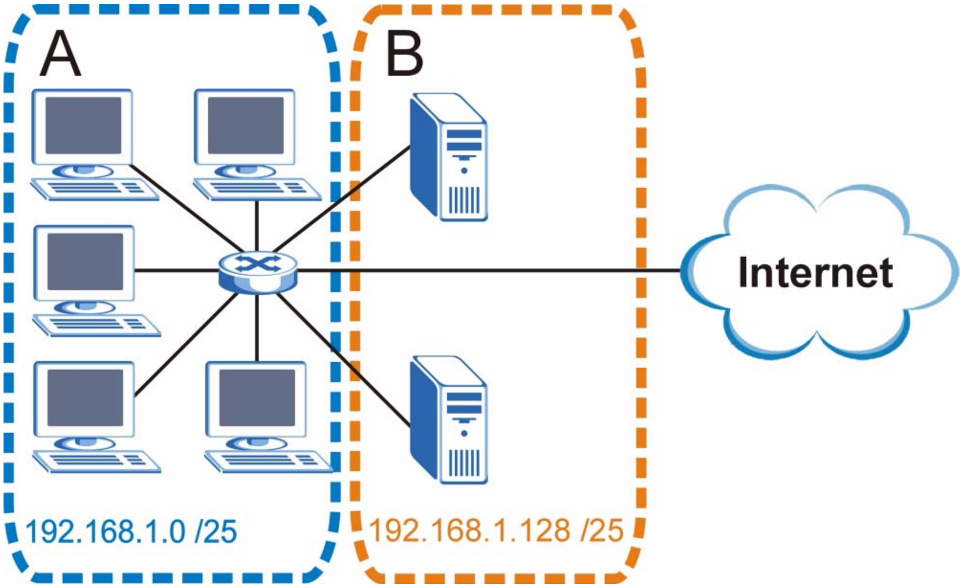


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.100.128 /25.

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

Figure 124 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 192.168.100.127 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 192.168.100.1 and the highest is 192.168.100.126.

Similarly, the host ID range for subnet **B** is 192.168.100.129 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.**11**000000) 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 76 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.100.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 77 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.100.127	Highest Host ID: 192.168.100.126	

Table 78 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.100.128	Lowest Host ID: 192.168.100.129	
Broadcast Address: 192.168.100.191	Highest Host ID: 192.168.100.190	

Table 79 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.100.192	Lowest Host ID: 192.168.100.193	
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 80 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 81 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 82 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

Table 82 16-bit Network Number Subnet Planning (continued)

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 MAX-207HW2R.

Once you have decided on the network number, pick an IP address for your MAX-207HW2R that is easy to remember (for instance, 192.168.100.1) 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 MAX-207HW2R will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the MAX-207HW2R unless you are instructed to do otherwise.

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.

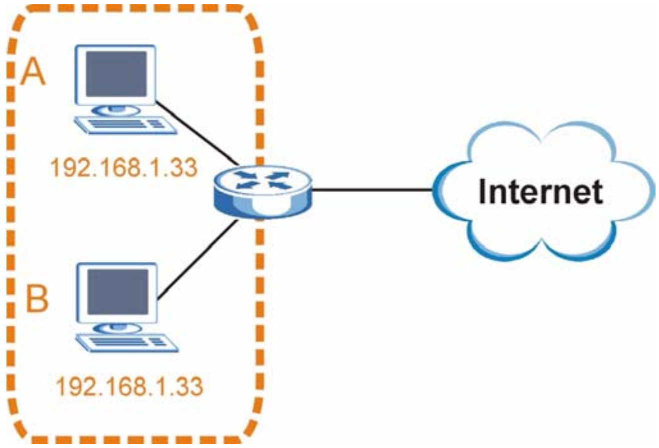
IP Address Conflicts

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.

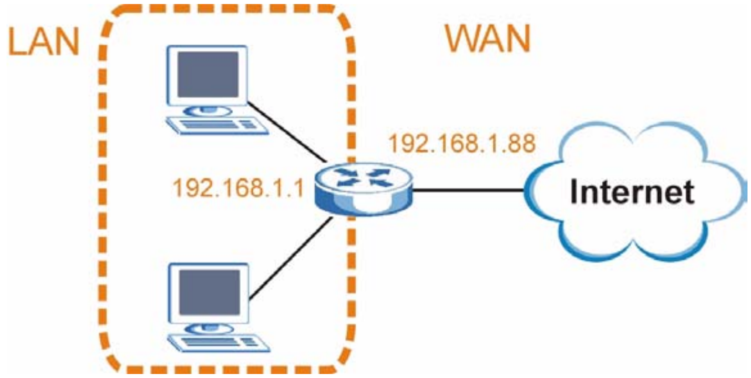
Figure 125 Conflicting Computer IP Addresses Example



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 126 Conflicting Computer IP Addresses Example

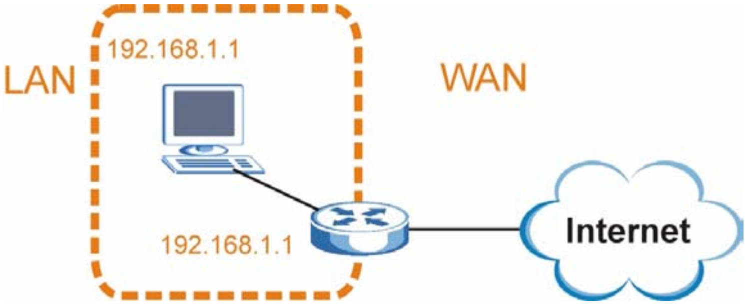


Conflicting Computer and Router IP Addresses Example

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 192.168.100.1 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 127 Conflicting Computer and Router IP Addresses Example



E

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.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These 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 ZyXEL-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:

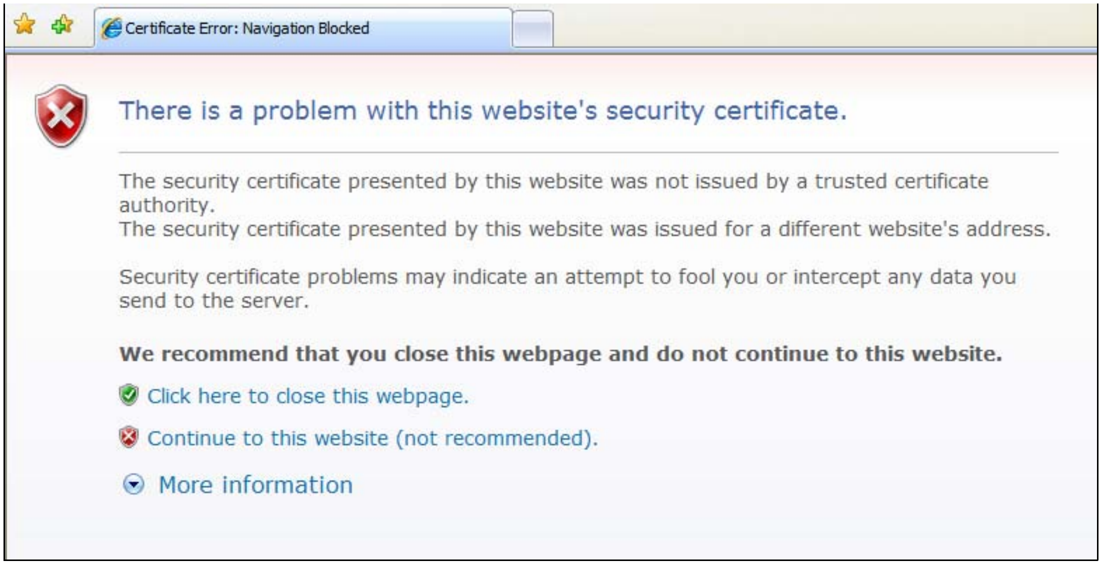
- Internet Explorer on page 238
- Firefox on page 248
- Opera on page 254
- Konqueror on page 262

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 128 Internet Explorer 7: Certification Error



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

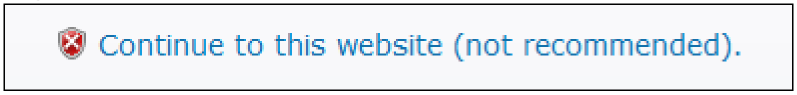
Click here to close this webpage.

Continue to this website (not recommended).

More information

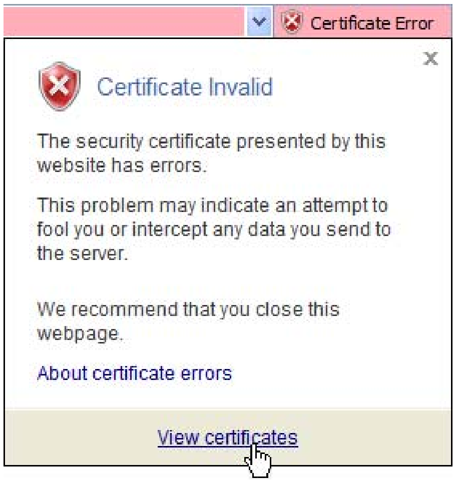
2 Click **Continue to this website (not recommended)**.

Figure 129 Internet Explorer 7: Certification Error



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

Figure 130 Internet Explorer 7: Certificate Error



The security certificate presented by this website has errors.

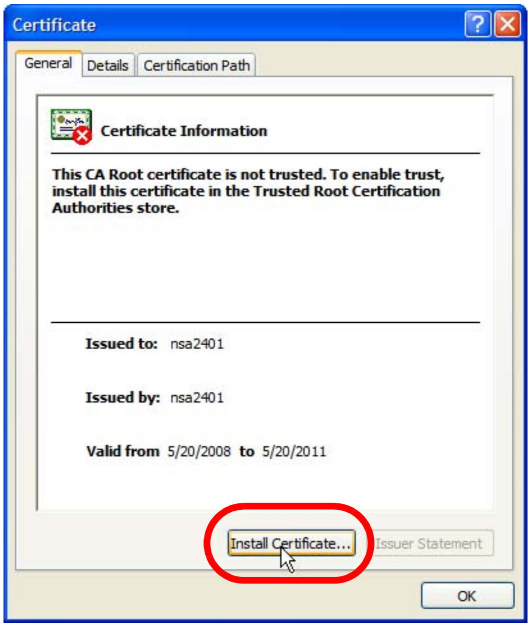
This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

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

Figure 131 Internet Explorer 7: Certificate



This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

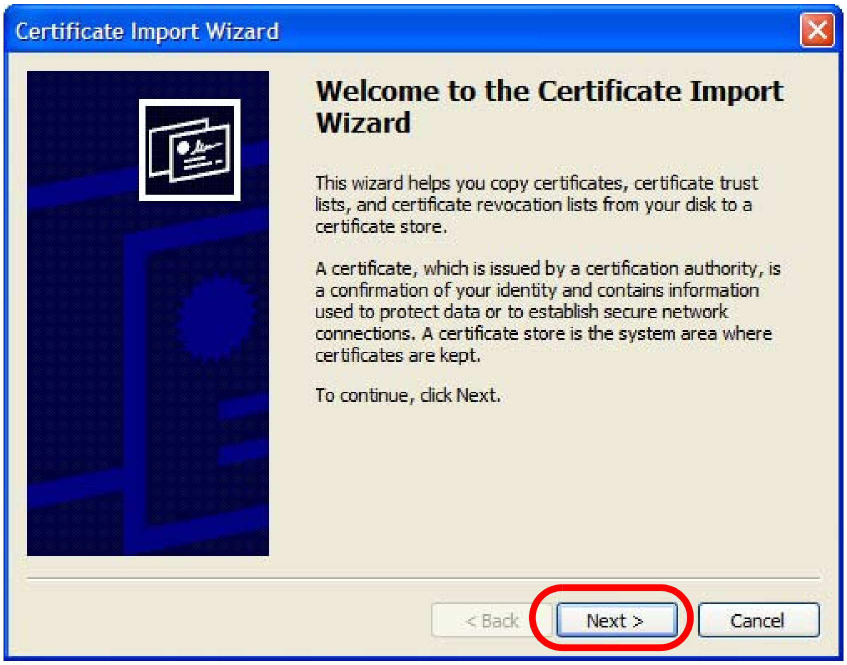
Issued to: nsa2401

Issued by: nsa2401

Valid from 5/20/2008 to 5/20/2011

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

Figure 132 Internet Explorer 7: Certificate Import Wizard



Certificate Import Wizard

Welcome to the Certificate Import Wizard

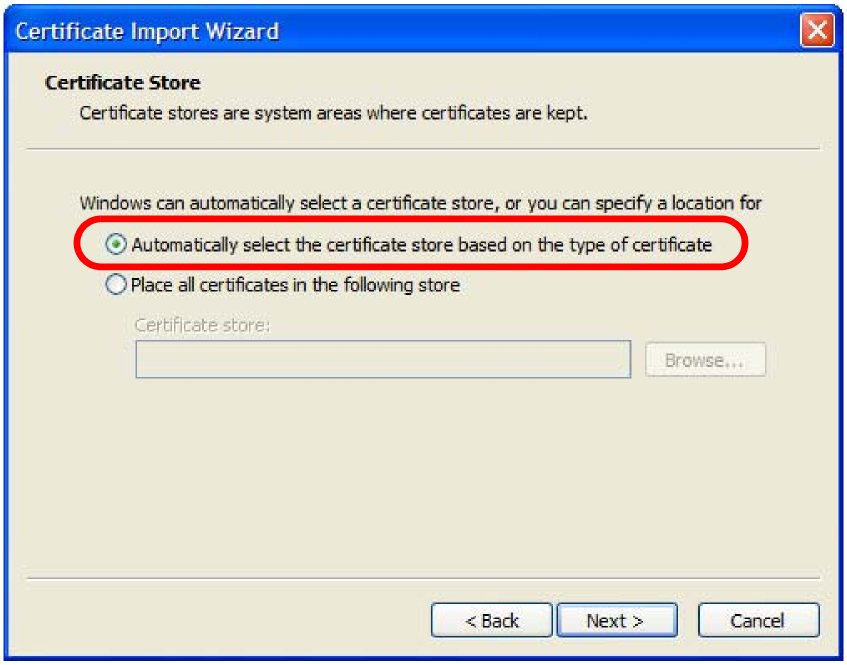
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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 133 Internet Explorer 7: Certificate Import Wizard



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

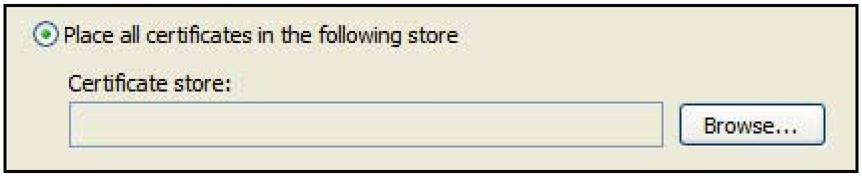
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

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

Figure 134 Internet Explorer 7: Certificate Import Wizard

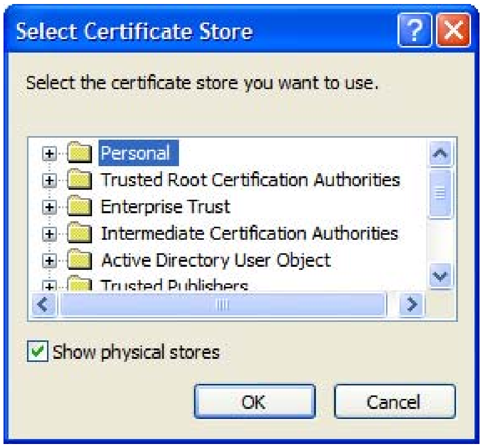


● Place all certificates in the following store

Certificate store:

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

Figure 135 Internet Explorer 7: Select Certificate Store



Select Certificate Store

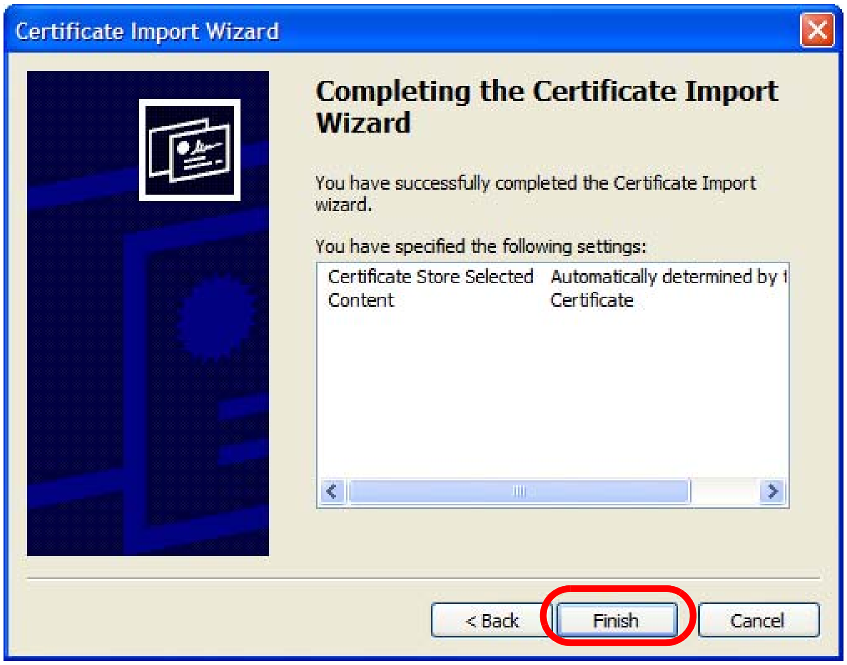
Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers

☑ Show physical stores

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

Figure 136 Internet Explorer 7: Certificate Import Wizard



Completing the Certificate Import Wizard

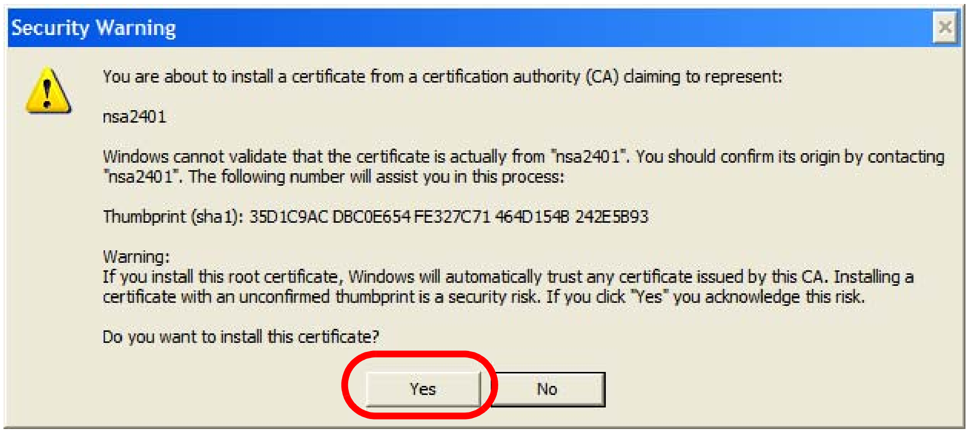
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

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

Figure 137 Internet Explorer 7: Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

nsa2401

Windows cannot validate that the certificate is actually from "nsa2401". You should confirm its origin by contacting "nsa2401". The following number will assist you in this process:

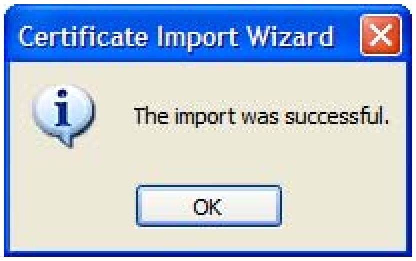
Thumbprint (sha1): 35D1C9AC DBC0E654 FE327C71 464D154B 242E5B93

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

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

Figure 138 Internet Explorer 7: Certificate Import Wizard

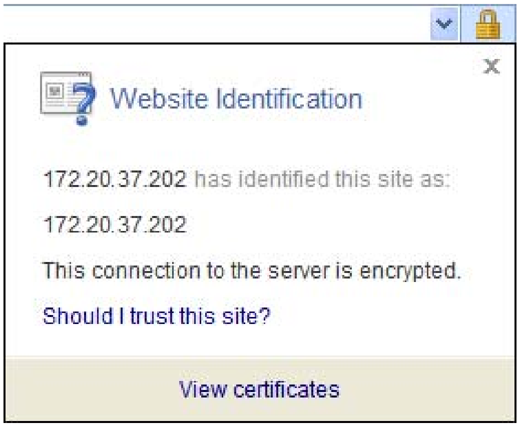


Certificate Import Wizard

The import was successful.

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

Figure 139 Internet Explorer 7: Website Identification



Website Identification

172.20.37.202 has identified this site as:

172.20.37.202

This connection to the server is encrypted.

Installing a Stand-Alone Certificate File in Internet Explorer

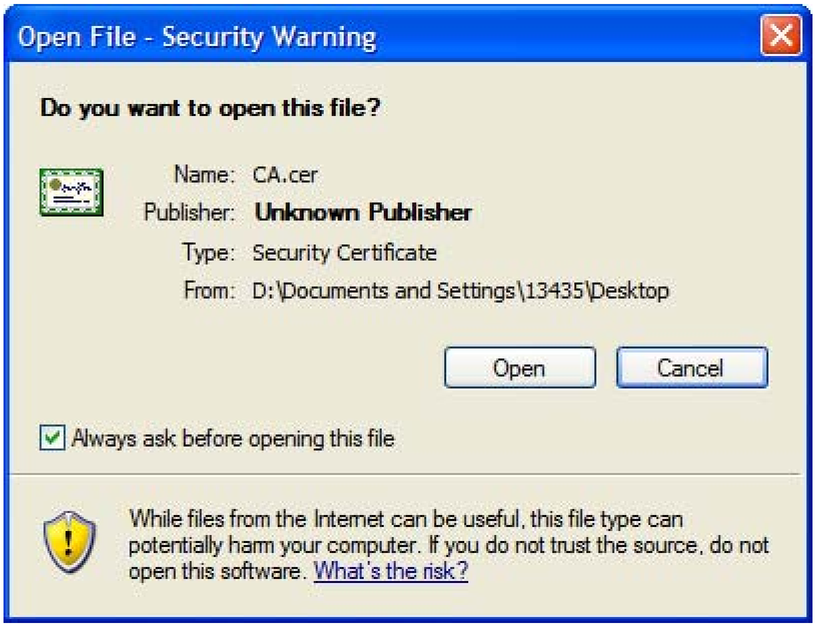
Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 140 Internet Explorer 7: Public Key Certificate File

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

Figure 141 Internet Explorer 7: Open File - Security Warning



Open File - Security Warning

Do you want to open this file?

Name: CA.cer
Publisher: **Unknown Publisher**
Type: Security Certificate
From: D:\Documents and Settings\13435\Desktop

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

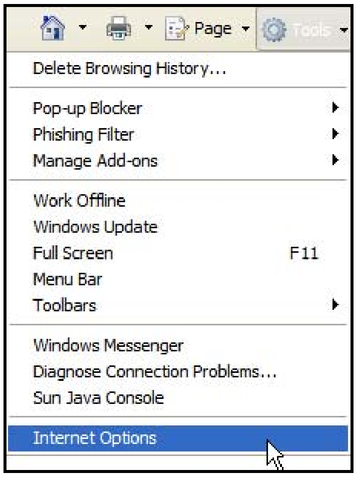
3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 238 to complete the installation process.

Removing a Certificate in Internet Explorer

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

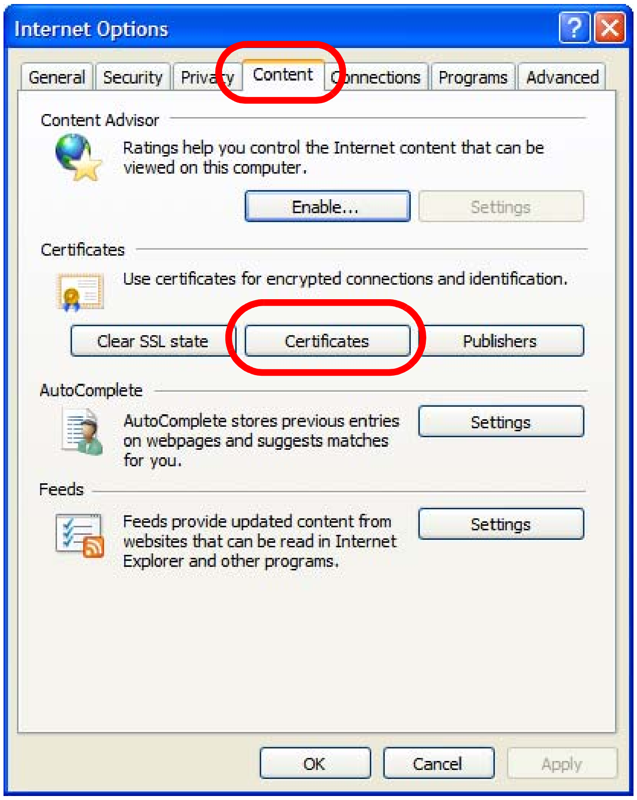
1 Open **Internet Explorer** and click **TOOLS > Internet Options**.

Figure 142 Internet Explorer 7: Tools Menu



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

Figure 143 Internet Explorer 7: Internet Options



Ratings help you control the Internet content that can be viewed on this computer.

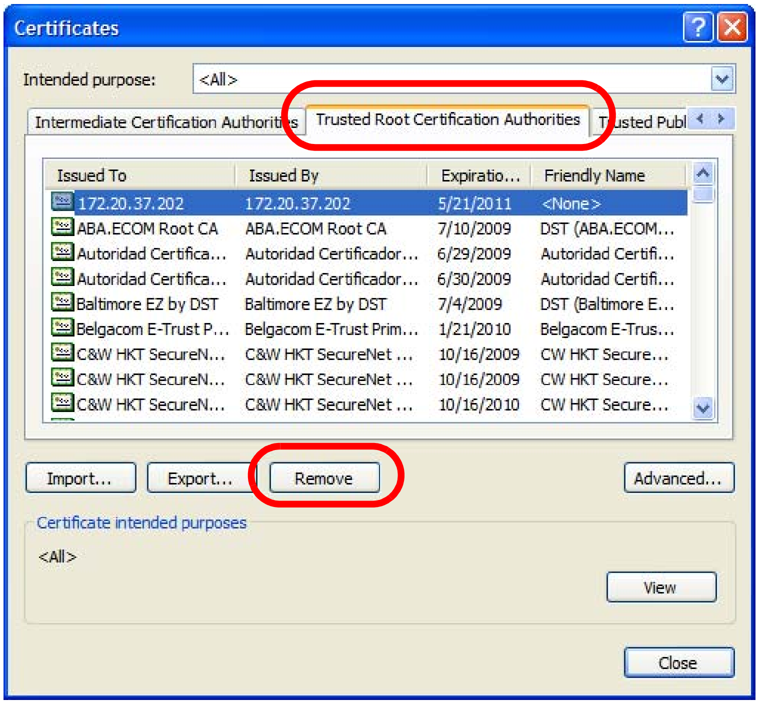
Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

3 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 144 Internet Explorer 7: Certificates



Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

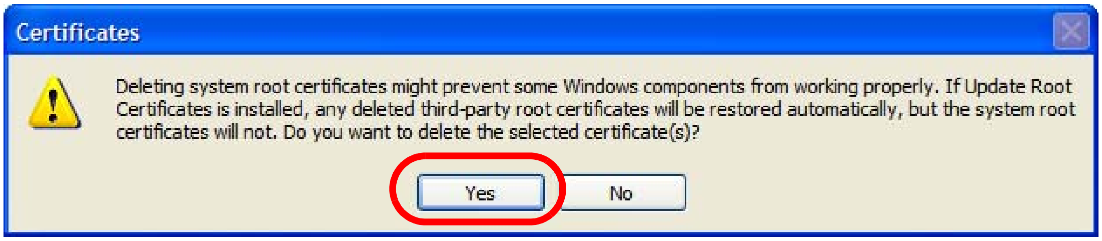
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
172.20.37.202	172.20.37.202	5/21/2011	<None>
ABA.ECOM Root CA	ABA.ECOM Root CA	7/10/2009	DST (ABA.ECOM...
Autoridad Certifica...	Autoridad Certificador...	6/29/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	6/30/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	7/4/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	1/21/2010	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2010	CW HKT Secure...

<All>

4 In the **Certificates** confirmation, click **Yes**.

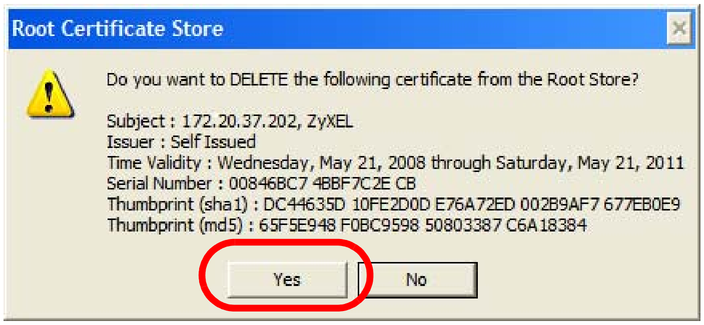
Figure 145 Internet Explorer 7: Certificates



Deleting system root certificates might prevent some Windows components from working properly. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?

5 In the **Root Certificate Store** dialog box, click **Yes**.

Figure 146 Internet Explorer 7: Root Certificate Store



Do you want to DELETE the following certificate from the Root Store?

Subject : 172.20.37.202, ZyXEL
Issuer : Self Issued
Time Validity : Wednesday, May 21, 2008 through Saturday, May 21, 2011
Serial Number : 00846BC7 4BBF7C2E CB
Thumbprint (sha1) : DC44635D 10FE2D0D E76A72ED 002B9AF7 677EB0E9
Thumbprint (md5) : 65F5E948 F0BC9598 50803387 C6A18384

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

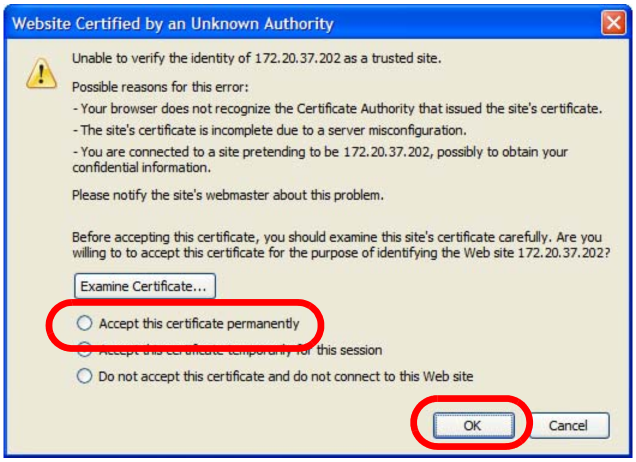
Firefox

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 147 Firefox 2: Website Certified by an Unknown Authority



Website Certified by an Unknown Authority

Unable to verify the identity of 172.20.37.202 as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be 172.20.37.202, possibly to obtain your confidential information.

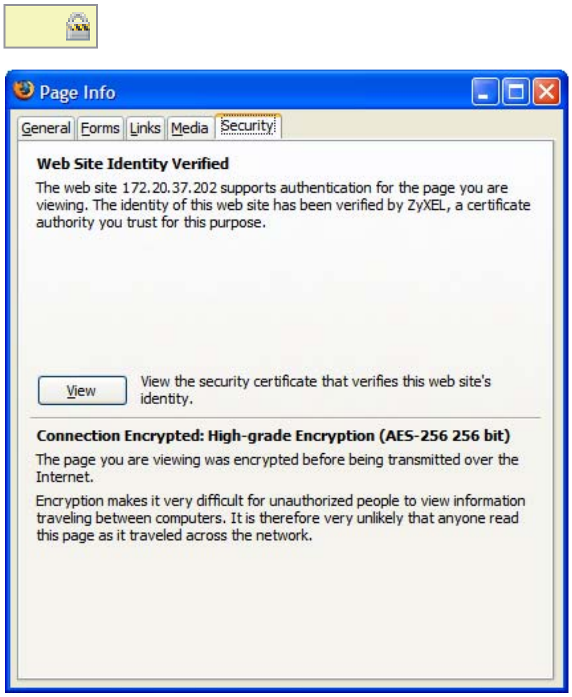
Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site 172.20.37.202?

Examine Certificate...
○ Accept this certificate permanently
○ Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this Web site
OK
Cancel

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 148 Firefox 2: Page Info



Web Site Identity Verified

The web site 172.20.37.202 supports authentication for the page you are viewing. The identity of this web site has been verified by ZyXEL, a certificate authority you trust for this purpose.

View the security certificate that verifies this web site's identity.

Connection Encrypted: High-grade Encryption (AES-256 256 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

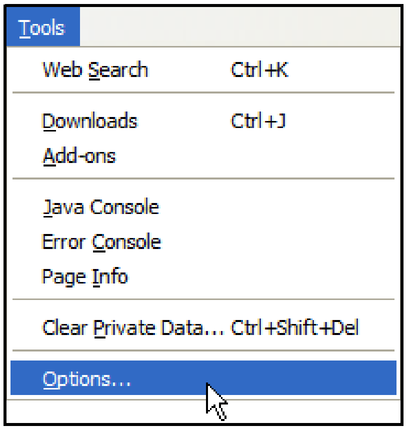
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL 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.

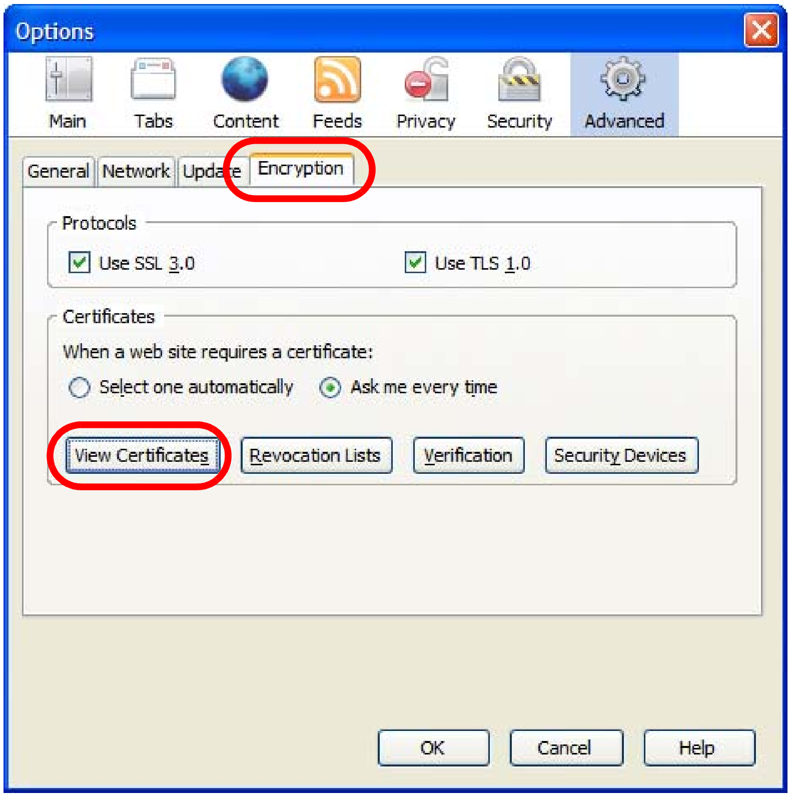
1 Open **Firefox** and click **TOOLS > Options**.

Figure 149 Firefox 2: Tools Menu



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

Figure 150 Firefox 2: Options



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

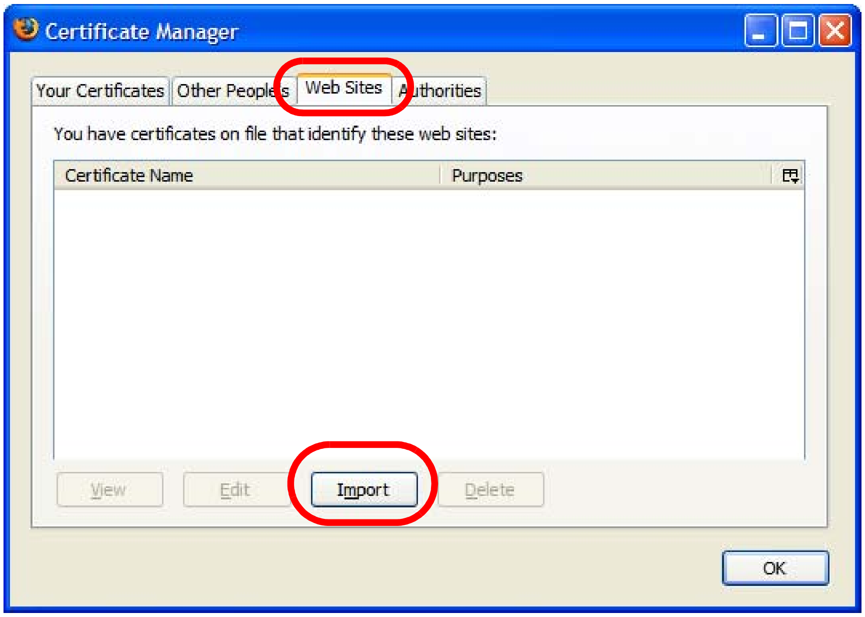
Certificates

When a web site requires a certificate:

○ Select one automatically ● Ask me every time

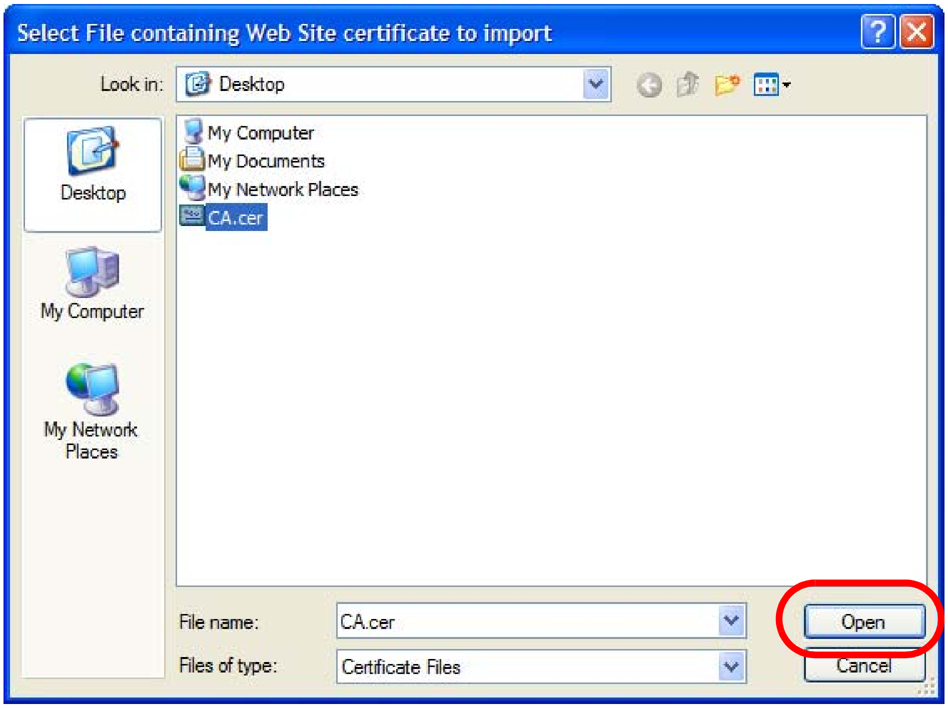
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

Figure 151 Firefox 2: Certificate Manager



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

Figure 152 Firefox 2: Select File



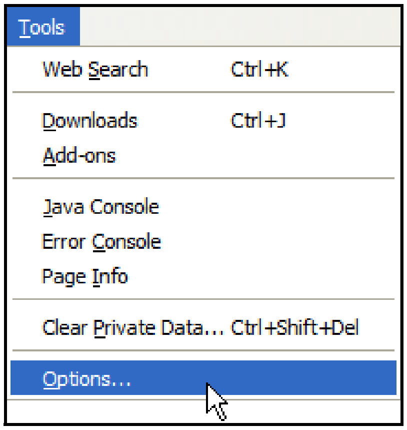
5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

Removing a Certificate in Firefox

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

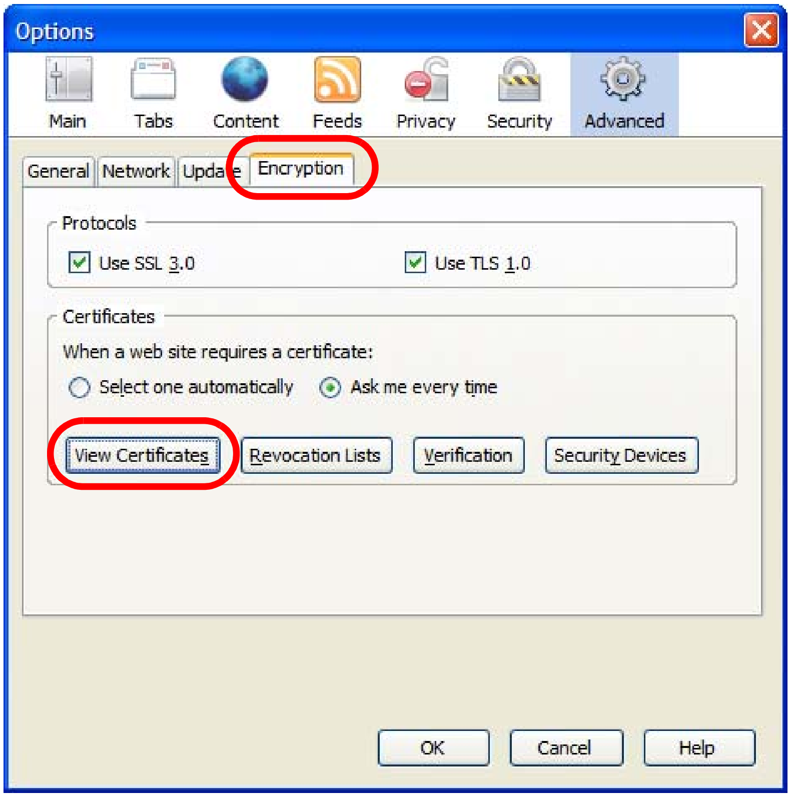
1 Open **Firefox** and click **TOOLS > Options**.

Figure 153 Firefox 2: Tools Menu



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

Figure 154 Firefox 2: Options



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

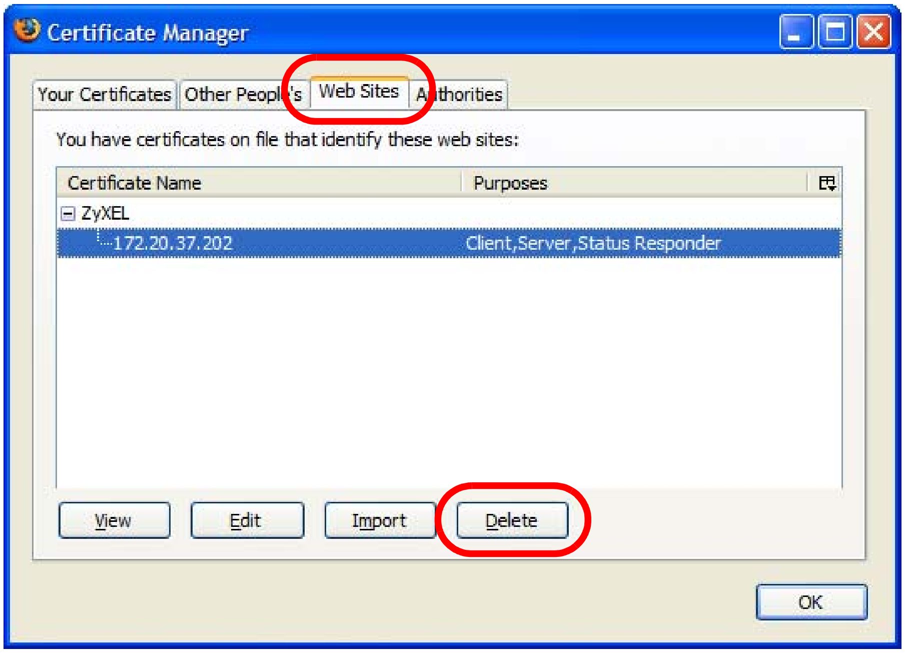
Certificates

When a web site requires a certificate:

○ Select one automatically ● Ask me every time

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 155 Firefox 2: Certificate Manager

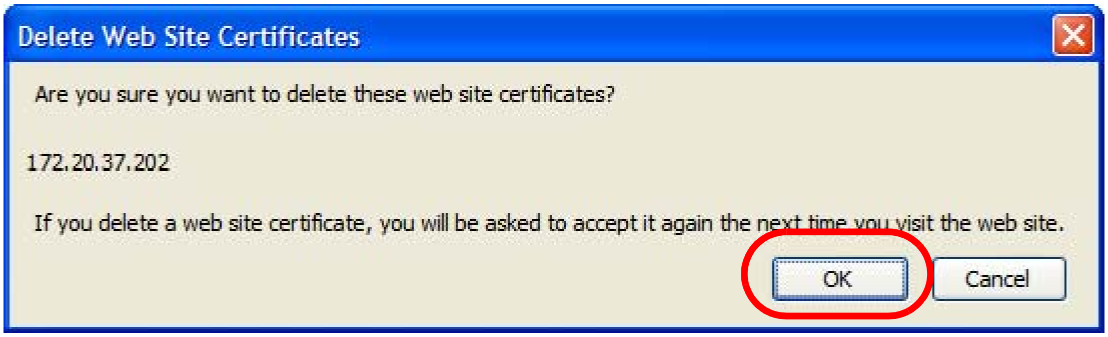


You have certificates on file that identify these web sites:

Certificate Name	Purposes
ZyXEL	
172.20.37.202	Client,Server,Status Responder

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

Figure 156 Firefox 2: Delete Web Site Certificates



Are you sure you want to delete these web site certificates?

172.20.37.202

If you delete a web site certificate, you will be asked to accept it again the next time you visit the web site.

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

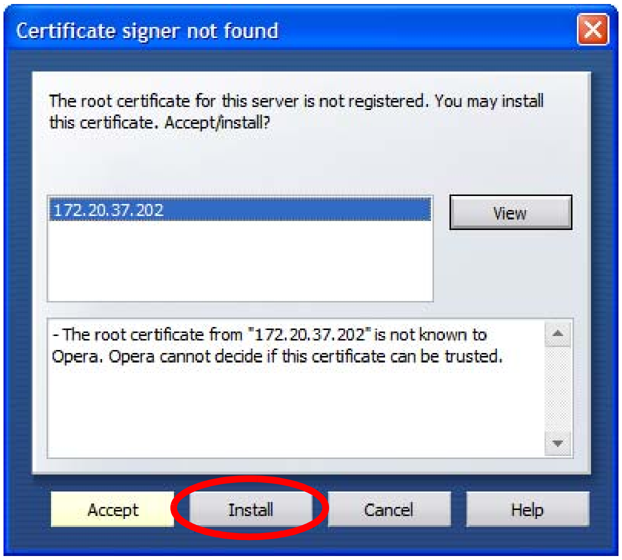
Opera

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 157 Opera 9: Certificate signer not found



Certificate signer not found

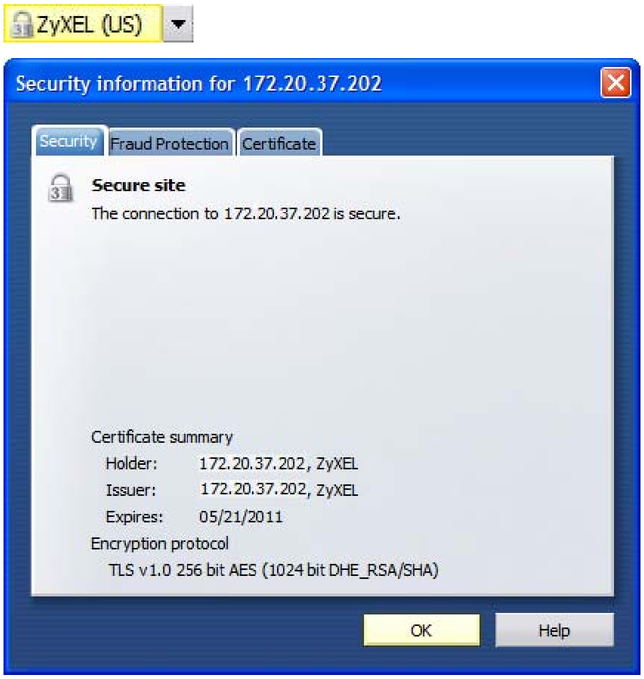
The root certificate for this server is not registered. You may install this certificate. Accept/install?

172.20.37.202

- The root certificate from "172.20.37.202" is not known to Opera. Opera cannot decide if this certificate can be trusted.

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 158 Opera 9: Security information



Secure site

The connection to 172.20.37.202 is secure.

Certificate summary

Holder:	172.20.37.202, ZyXEL
Issuer:	172.20.37.202, ZyXEL
Expires:	05/21/2011

Encryption protocol

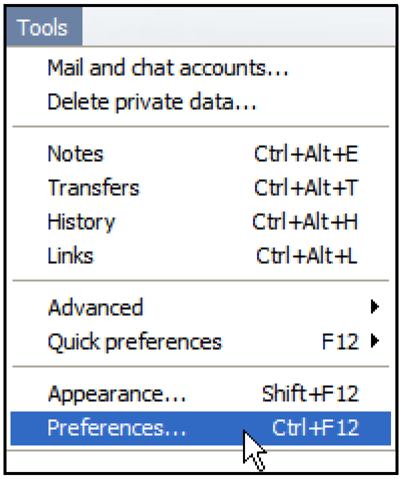
TLS v1.0 256 bit AES (1024 bit DHE_RSA/SHA)

Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL 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.

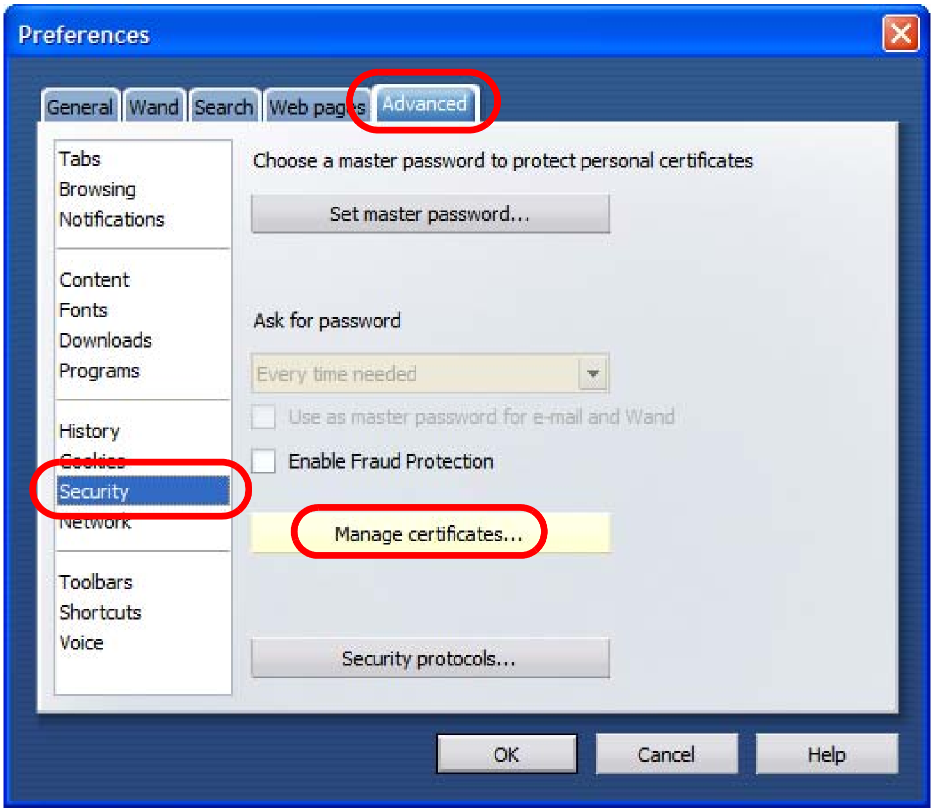
1 Open **Opera** and click **TOOLS > Preferences**.

Figure 159 Opera 9: Tools Menu



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

Figure 160 Opera 9: Preferences



Choose a master password to protect personal certificates

Ask for password

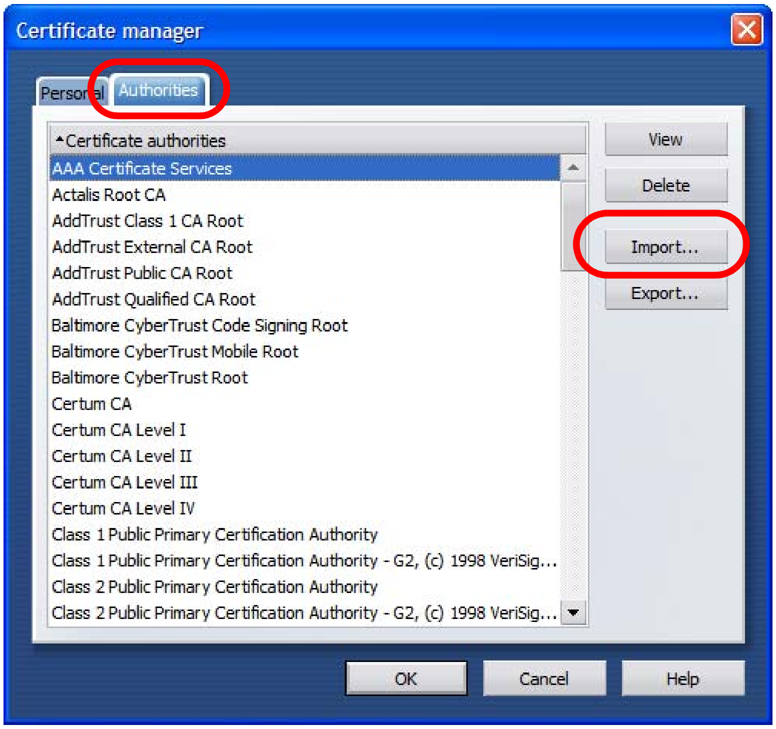
Every time needed

□ Use as master password for e-mail and Wand

□ Enable Fraud Protection

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

Figure 161 Opera 9: Certificate manager

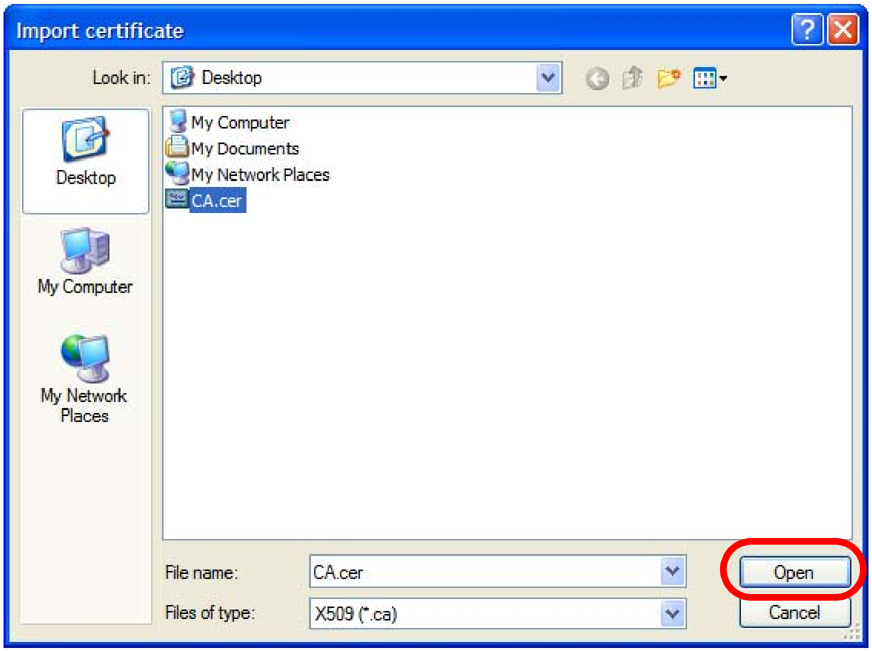


Certificate authorities

- AAA Certificate Services
- Actalis Root CA
- AddTrust Class 1 CA Root
- AddTrust External CA Root
- AddTrust Public CA Root
- AddTrust Qualified CA Root
- Baltimore CyberTrust Code Signing Root
- Baltimore CyberTrust Mobile Root
- Baltimore CyberTrust Root
- Certum CA
- Certum CA Level I
- Certum CA Level II
- Certum CA Level III
- Certum CA Level IV
- Class 1 Public Primary Certification Authority
- Class 1 Public Primary Certification Authority - G2, (c) 1998 VeriSig...
- Class 2 Public Primary Certification Authority
- Class 2 Public Primary Certification Authority - G2, (c) 1998 VeriSig...

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

Figure 162 Opera 9: Import certificate



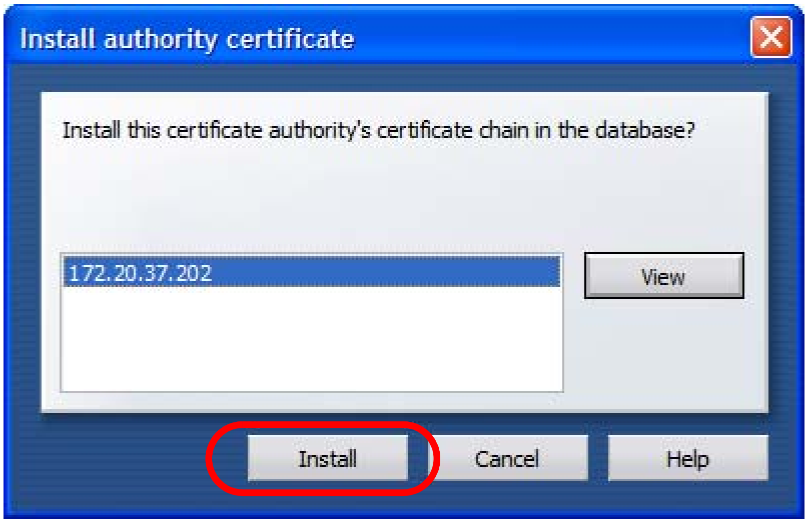
Look in: Desktop

File name: CA.cer

Files of type: X509 (*.ca)

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

Figure 163 Opera 9: Install authority certificate



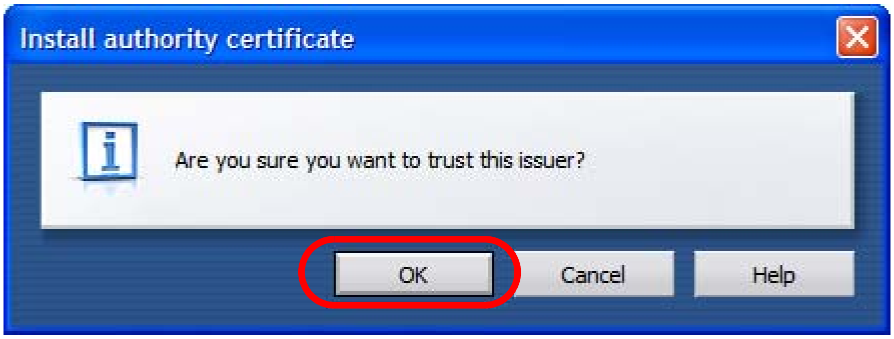
Install authority certificate

Install this certificate authority's certificate chain in the database?

172.20.37.202

6 Next, click **OK**.

Figure 164 Opera 9: Install authority certificate



Install authority certificate

Are you sure you want to trust this issuer?

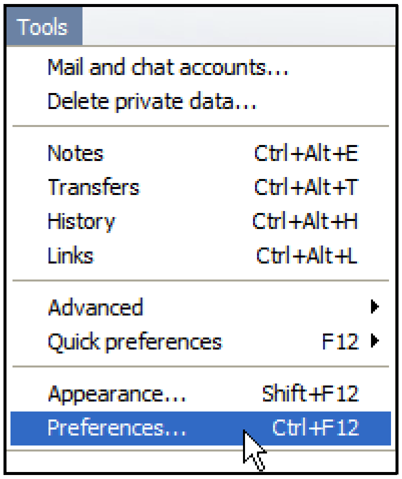
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

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

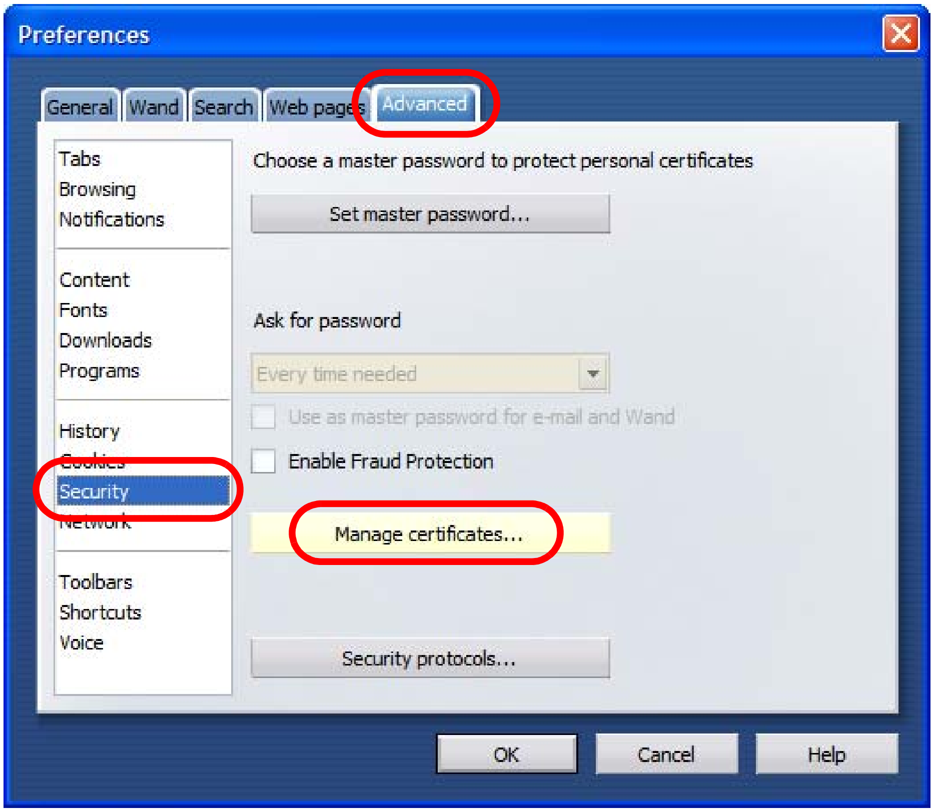
1 Open **Opera** and click **TOOLS > Preferences**.

Figure 165 Opera 9: Tools Menu



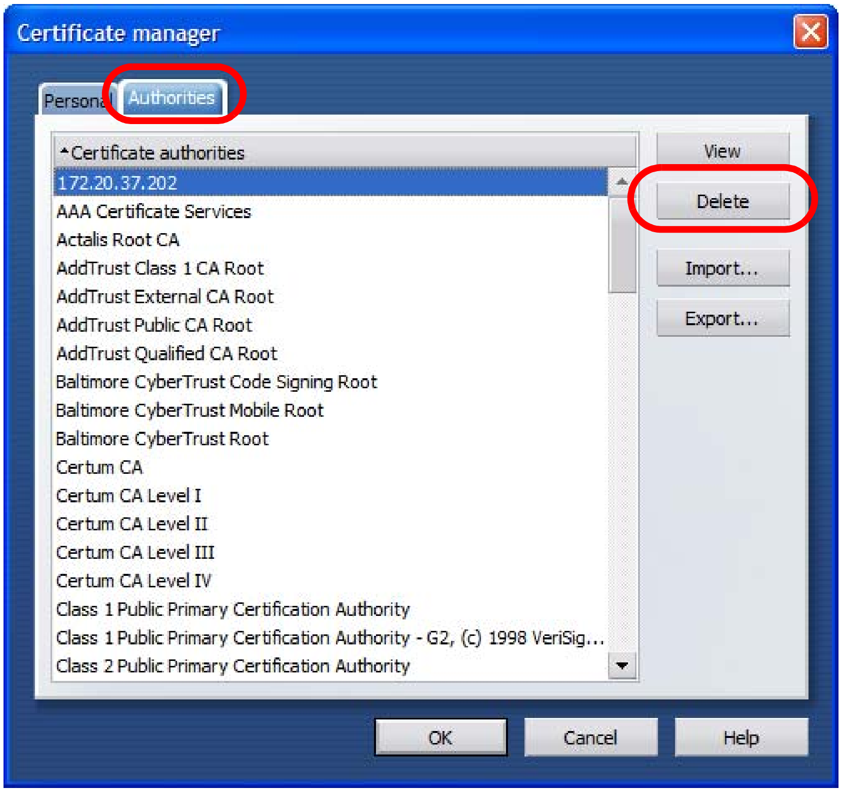
2 In **Preferences**, **ADVANCED > Security** > **Manage certificates**.

Figure 166 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 167 Opera 9: Certificate manager



Certificate authorities

172.20.37.202
AAA Certificate Services
Actalis Root CA
AddTrust Class 1 CA Root
AddTrust External CA Root
AddTrust Public CA Root
AddTrust Qualified CA Root
Baltimore CyberTrust Code Signing Root
Baltimore CyberTrust Mobile Root
Baltimore CyberTrust Root
Certum CA
Certum CA Level I
Certum CA Level II
Certum CA Level III
Certum CA Level IV
Class 1 Public Primary Certification Authority
Class 1 Public Primary Certification Authority - G2, (c) 1998 VeriSig...
Class 2 Public Primary Certification Authority

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.

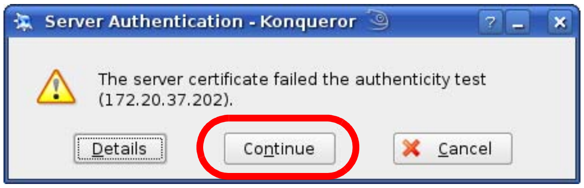
Konqueror

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**.

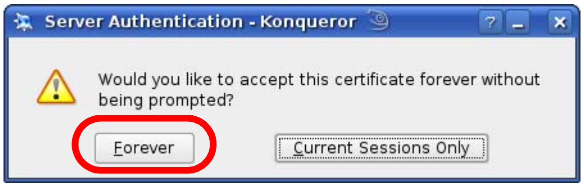
Figure 168 Konqueror 3.5: Server Authentication



The server certificate failed the authenticity test (172.20.37.202).

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

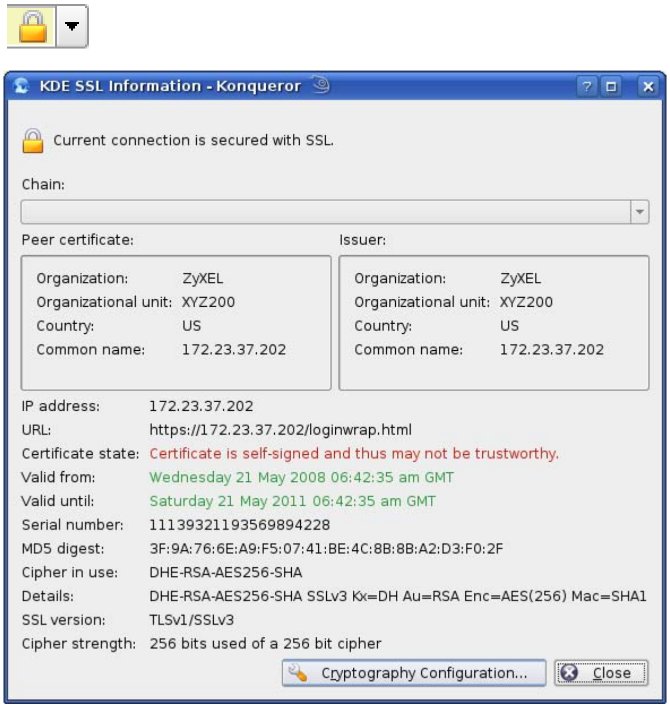
Figure 169 Konqueror 3.5: Server Authentication



Would you like to accept this certificate forever without being prompted?

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

Figure 170 Konqueror 3.5: KDE SSL Information



Current connection is secured with SSL.

Chain:

Peer certificate:		Issuer:	
Organization:	ZyXEL	Organization:	ZyXEL
Organizational unit:	XYZ200	Organizational unit:	XYZ200
Country:	US	Country:	US
Common name:	172.23.37.202	Common name:	172.23.37.202

IP address:	172.23.37.202
URL:	https://172.23.37.202/loginwrap.html
Certificate state:	Certificate is self-signed and thus may not be trustworthy.
Valid from:	Wednesday 21 May 2008 06:42:35 am GMT
Valid until:	Saturday 21 May 2011 06:42:35 am GMT
Serial number:	11139321193569894228
MD5 digest:	3F:9A:76:6E:A9:F5:07:41:BE:4C:8B:8B:A2:D3:F0:2F
Cipher in use:	DHE-RSA-AES256-SHA
Details:	DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
SSL version:	TLSv1/SSLv3
Cipher strength:	256 bits used of a 256 bit cipher

Installing a Stand-Alone Certificate File in Konqueror

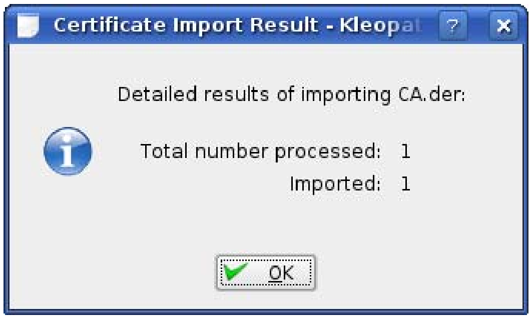
Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 171 Konqueror 3.5: Public Key Certificate File

2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

Figure 172 Konqueror 3.5: Certificate Import Result

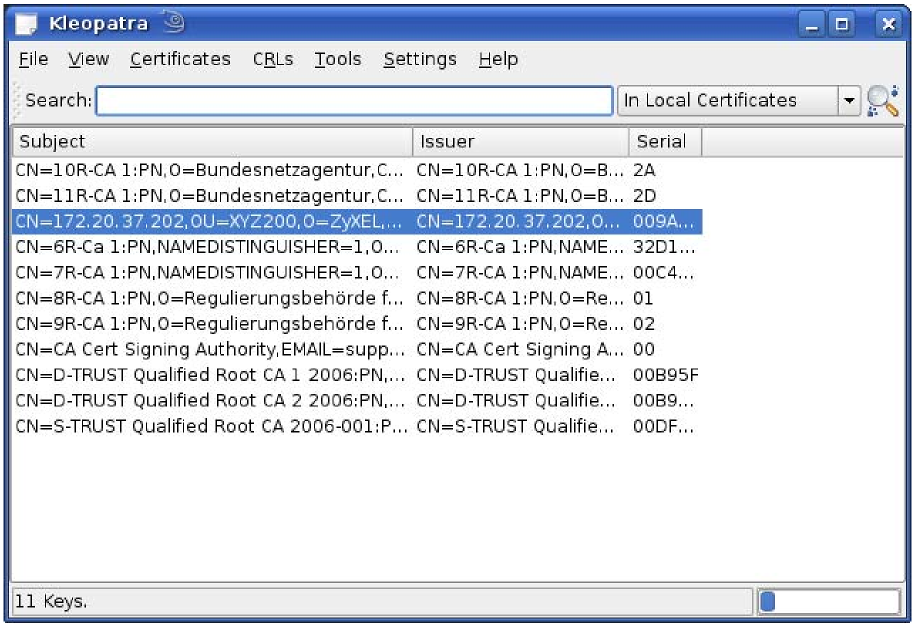


Detailed results of importing CA.der:

Total number processed: 1
Imported: 1

The public key certificate appears in the KDE certificate manager, **Kleopatra**.

Figure 173 Konqueror 3.5: Kleopatra



Subject	Issuer	Serial
CN=10R-CA 1:PN,O=Bundesnetzagentur,C...	CN=10R-CA 1:PN,O=B...	2A
CN=11R-CA 1:PN,O=Bundesnetzagentur,C...	CN=11R-CA 1:PN,O=B...	2D
CN=172.20.37.202,OU=XYZ200,O=ZyXEL,...	CN=172.20.37.202,O...	009A...
CN=6R-Ca 1:PN,NAMEDISTINGUISHER=1,O...	CN=6R-Ca 1:PN,NAME...	32D1...
CN=7R-CA 1:PN,NAMEDISTINGUISHER=1,O...	CN=7R-CA 1:PN,NAME...	00C4...
CN=8R-CA 1:PN,O=Regulierungsbehörde f...	CN=8R-CA 1:PN,O=Re...	01
CN=9R-CA 1:PN,O=Regulierungsbehörde f...	CN=9R-CA 1:PN,O=Re...	02
CN=CA Cert Signing Authority,EMAIL=supp...	CN=CA Cert Signing A...	00
CN=D-TRUST Qualified Root CA 1 2006:PN,...	CN=D-TRUST Qualifie...	00B95F
CN=D-TRUST Qualified Root CA 2 2006:PN,...	CN=D-TRUST Qualifie...	00B9...
CN=S-TRUST Qualified Root CA 2006-001:P...	CN=S-TRUST Qualifie...	00DF...

11 Keys.

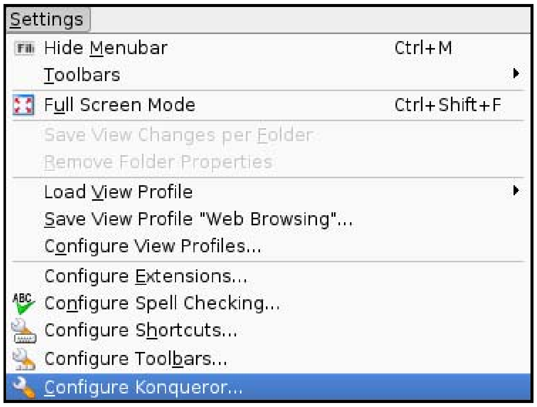
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

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**.

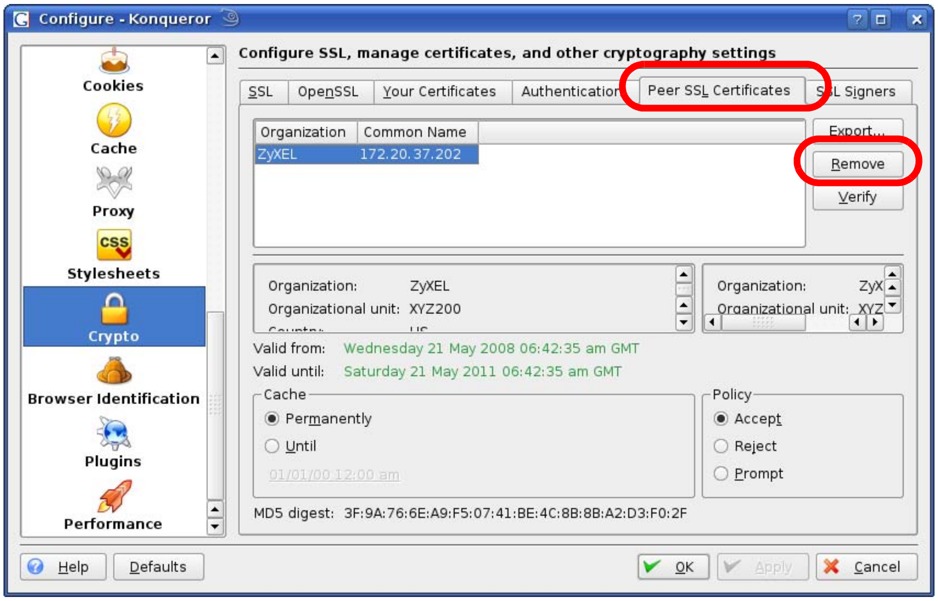
Figure 174 Konqueror 3.5: Settings Menu



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 175 Konqueror 3.5: Configure



Configure SSL, manage certificates, and other cryptography settings

Organization	Common Name
ZyXEL	172.20.37.202

Organization: ZyXEL
Organizational unit: XYZ200

Organization: ZyX
Organizational unit: XYZ

Valid from: Wednesday 21 May 2008 06:42:35 am GMT
Valid until: Saturday 21 May 2011 06:42:35 am GMT

Cache
● Permanently
○ Until
01/01/00 12:00 am

Policy
● Accept
○ Reject
○ Prompt

MD5 digest: 3F:9A:76:6E:A9:F5:07:41:BE:4C:8B:8B:A2:D3:F0:2F

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.

F

SIP Passthrough

Enabling/Disabling the SIP ALG

You can turn off the MAX-207HW2R SIP ALG to avoid retranslating the IP address of an existing SIP device that is using STUN. If you want to use STUN with a SIP client device (a SIP phone or IP phone for example) behind the MAX-207HW2R, use the `ip alg disable ALG_SIP` command to turn off the SIP ALG.

Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP UA sends registration packets to the SIP server periodically and keeps the session alive in the MAX-207HW2R.

If the SIP client does not have this mechanism and makes no call during the MAX-207HW2R SIP timeout default (60 minutes), the MAX-207HW2R SIP ALG drops any incoming calls after the timeout period. You can use the `ip alg siptimeout` command to change the timeout value.

Audio Session Timeout

If no voice packets go through the SIP ALG before the timeout period default (5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

G

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 83 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 (for example www.zyxel.com) to IP numbers.

Table 83 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
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 83 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 83 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.

H

Legal Information

Copyright

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the MAX-207HW2R is subject to the terms and conditions of any related service providers.

Do not use the MAX-207HW2R for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device 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 device 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 device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index