9

The VoIP General Screens

9.1 VoIP Overview

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

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

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

9.1.1 What You Can Do in This Chapter

- The **Media** screen (Section 9.2 on page 159) lets you set up and maintain global VoIP settings on the BM2022w.
- The **QoS** screen (Section 9.3 on page 160) lets you set up and maintain QoS settings for voice traffic flowing through the BM2022w.
- The **SIP** screen (Section 9.4 on page 161) lets you enable session timer and select the SIP session refresh method.
- The **Speed Dial** screen (Section 9.5 on page 161) lets you add, edit, or remove speed-dial entries for the phone line.

9.1.2 What You Need to Know

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

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The BM2022w supports the following codecs.

- **G.711** is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals (sampling) and converts them into digital bits (quantization). Quantization “reads” the analog signal and then “writes” it to the nearest digital value. For this reason, a digital sample is usually slightly different from its analog original (this difference is known as “quantization noise”). G.711 provides excellent sound quality but requires 64kbps of bandwidth.

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

Quality of Service (QoS)

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

Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the BM2022w) so a server can decide the best method of delivery, that is the least cost, fastest route and so on. The ToS field is consist of 8 bits. The first 3 bits indicate the priority of the packet.

DiffServ

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

DiffServ uses the first 6 bits of the 8-bit ToS value so that it can be backward compatible with non-DiffServ compliant but ToS-enabled network device. See Section 9.6.1 on page 162 for more information.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

RTP

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

Speed Dial

Speed dial provides shortcuts for dialing frequently used phone numbers. You can map a phone number to a self-defined key(s) and then use that key(s) to call the phone number. For example, you can map 123456 to #01. When you press #01 it means that you press 123456.

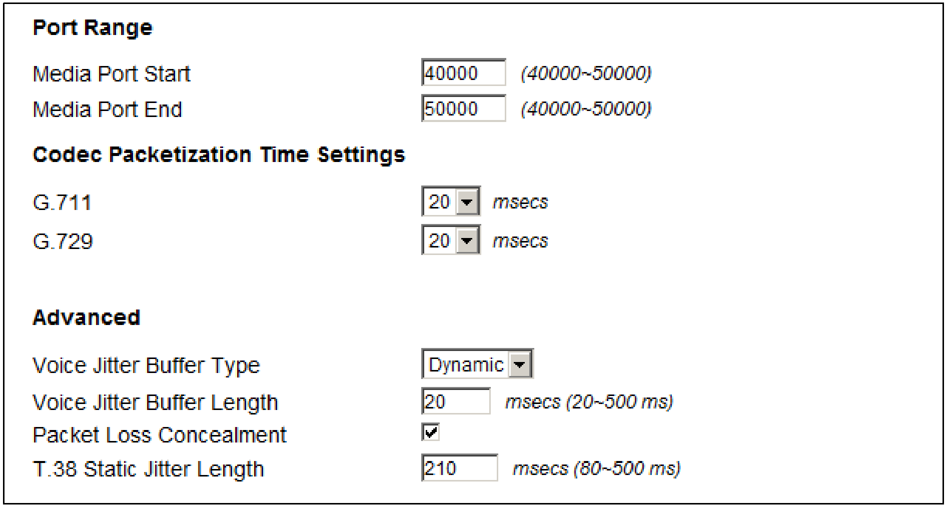
9.1.3 Before you Begin

- Ensure that you have all of your voice account information on hand. If not, contact your voice account service provider to find out which settings in this chapter you should configure in order to use your telephone with the BM2022w.
- Connect your BM2022w to the Internet, as described in the Quick Start Guide. If you have not already done so, then you will not be able to test your VoIP settings.

9.2 Media

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

Figure 86 VoIP > General > Media



Port Range

Media Port Start 40000 (40000~50000)

Media Port End 50000 (40000~50000)

Codec Packetization Time Settings

G.711 20 msecs

G.729 20 msecs

Advanced

Voice Jitter Buffer Type Dynamic

Voice Jitter Buffer Length 20 msecs (20~500 ms)

Packet Loss Concealment ☑

T.38 Static Jitter Length 210 msecs (80~500 ms)

The following table describes the labels in this screen.

Table 68 VoIP > General > Media

LABEL	DESCRIPTION
Port Range	
Media Port Start Media Port End	Enter the listening port number(s) for RTP traffic on the BM2022w, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the both **Media Port Start** and **Media Port End** fields. To enter a range of ports, enter the beginning port number of the range in the **Media Port Start** field and the ending port number in the **Media Port End** field.
Codec Packetization Time Settings	
G.711, G.729	Select how often (**10** to **60** msecs) the BM2022w sends an RTP packet for each type of voice coder/decoder (codec) **G.711** and **G.729**.
Advanced	

Table 68 VoIP > General > Media (continued)

LABEL	DESCRIPTION
Voice Jitter Buffer Type	Voice jitter is a variation in delay of RTP packets delivery. This could cause strange sound effects. The BM2022w can utilize the following types of jitter buffer to minimize the effects of jitter. **Dynamic** - Jitter buffer size is dynamically changed by RTP packets delivery status. **Static** - Jitter buffer size is fixed.
Voice Jitter Buffer Length	Select the maximum number of milliseconds of voice traffic the BM2022w can help to smooth out the jitter in order to ensure good voice quality for your conversations.
Packet Loss Concealment	Packets may be dropped due to an overwhelming amount of traffic on the network. Some degree of packet loss will not be noticeable to the end user, but as packet loss increases the quality of sound degrades. Select this to have the BM2022w to improve the voice quality when packet loss occurs.
T.38 Static Jitter Length	T.38 is an ITU-T standard that VoIP devices use to send fax messages over the Internet. Select the number of milliseconds for the jitter buffer size used for transmitting T.38 fax messages.

9.3 QoS

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

Click **VoIP > General > QoS** to set up Type of Service (ToS) and Differentiated Services (Diffserv) settings for voice traffic transmission through the BM2022w.

Figure 87 VoIP > General > QoS

SIP ToS / DiffServ 0x2E

RTP ToS / DiffServ 0x38

The following table describes the labels in this screen.

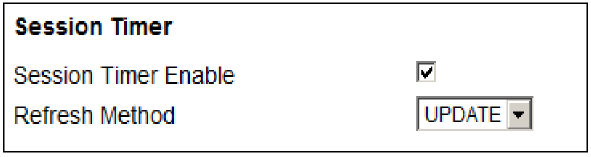
Table 69 VoIP > General > QoS

LABEL	DESCRIPTION
SIP ToS/DiffServ	Enter the DSCP value you want to mark on all outgoing SIP packets generated by the BM2022w for DiffServ-enabled networks. Since DiffServ uses the first 6 bits of the 8-bit IP ToS field to represent the DSCP value, enter here the 6-bit DSCP value you want to mark in hexadecimal (in a format of 0x00), and the BM2022w will then automatically append 2 bits '0' to make a whole 8-bit ToS field value for all outgoing SIP packets. For example, if you enter 0x2E, it is 101110 in binary for DSCP. The BM2022w converts it to 10111000 in binary and marks on the IP ToS field of all the outgoing SIP packets.
RTP ToS/DiffServ	Enter the DSCP value you want to mark on all outgoing VoIP data packets (including both RTP and T.38 UDPTL packets) generated by the BM2022 for DiffServ-enabled networks.

9.4 SIP Settings

Click **VoIP > General > SIP** to set up session timer on the BM2022w. See Section 10.8 on page 173 for more information on SIP.

Figure 88 VoIP > General > SIP



Session Timer

Session Timer Enable ☑

Refresh Method UPDATE

The following table describes the labels in this screen.

Table 70 VoIP > General > SIP

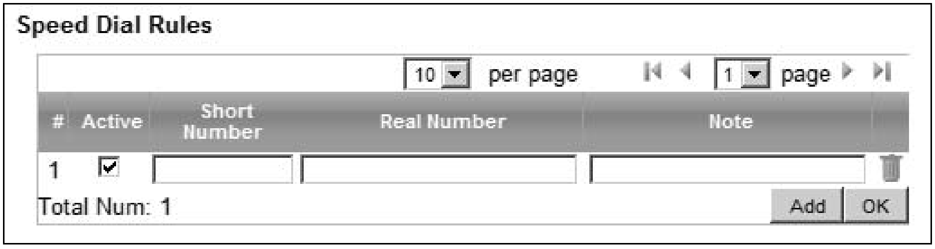
LABEL	DESCRIPTION
Session Timer Enable	Select this to activate the BM2022w's SIP Session Timer. SIP Session Timer is a function used by both of the communication peers to determine if the call session is still active (alive) or not. It uses the method specified in the following **Refresh Method** field to periodically refresh the SIP sessions.
Refresh Method	Select the method to be used for periodically refreshing SIP sessions, to determine if the session is still active. Select **UPDATE** to use Update requests to refresh the session and select **INVITE** to use Re-Invite requests. You should use the same method as the peer device. The Update method uses less overhead than Re-Invite, but is not as widely supported as Re-Invite. By default the BM2022w is set to use the **UPDATE** method. When set to **UPDATE**, the BM2022w can also revert to using the **INVITE** method for SIP session refresh, depending on the method supported and allowed by the peer device.

9.5 Speed Dial

Speed dial allows you to use a shorter number for dialing frequently used phone numbers.

Click **VoIP > General > Speed Dial** to add, edit, or remove speed-dial rules.

Figure 89 VoIP > General > Speed Dial



Speed Dial Rules

10 per page 1 page

#	Active	Short Number	Real Number	Note	
1	☑				

Total Num: 1

The following table describes the labels in this screen.

Table 71 VoIP > General > Speed Dial

LABEL	DESCRIPTION
Speed Dial Rules - This is a list of speed dial numbers. To edit an existing speed dial rule, you can click the row for the rule and editable fields will appear.	
Active	This field displays whether the rule is activated or not.
Short Number	This field displays the abbreviated number you want to use to substitute for the real (actual) phone number in the following **Real Number** field. When the rule is activated, you can press the assigned **Short Number** to dial the **Real Number**.
Real Number	This field displays the actual phone number you want the BM2022w to call when you use the specified **Short Number**. Enter the actual phone number you want the BM2022w to call when you use the specified **Short Number** if you are editing the entry.
Notes	This field displays additional information for this speed-dial rule. Enter additional information or any remark for this speed-dial rule if your are editing the entry.
Remove	Click this to remove the rule.
Add	Click this to add a new speed-dial rule.
OK	Click this to save the changes you made in this table.

9.6 Technical Reference

The following section contains additional technical information about the BM2022w features described in this chapter.

9.6.1 DSCP and Per-Hop Behavior

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

Figure 90 DiffServ: Differentiated Service Field

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

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

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

10

The VoIP Account Screens

10.1 Overview

Use the **VoIP > Account 1** and **VoIP > Account 2** screens to configure SIP servers, authentication, additional VoIP features, dialing timeout values and how to handle fax messages for two accounts on the BM2022w. Account 1 maps to phone port 1 and account 2 maps to phone port 2. Since both the **Account 1** and **Account 2** screens are quite similar, this section uses the **VoIP > Account 1** screens to describe the fields.

10.1.1 What You Can Do in This Chapter

- The **Status** screen (Section 10.2 on page 166) lets you view the current status of the SIP server, and selected phone line and call history. You can also manually disconnect the VoIP connection or request the SIP server for a new connection.
- The **Server** screen (Section 10.3 on page 168) lets you configure the SIP server, proxy server and outbound server settings for the phone line.
- The **SIP** screen (Section 10.4 on page 169) lets you configure the SIP account, codec and SIP settings for the phone line.
- The **Feature** screen (Section 10.5 on page 171) lets you configure the SIP additional functions such as DTMF, call forward and call waiting for the phone line.
- The **Dialing** screen (Section 10.6 on page 172) lets you configure some timeout setting for the phone line.
- The **FAX** screen (Section 10.7 on page 173) lets you configure which standard the phone line uses for sending faxes.

10.1.2 What You Need to Know

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

SIP Identities

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

SIP Number

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

SIP Service Domain

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

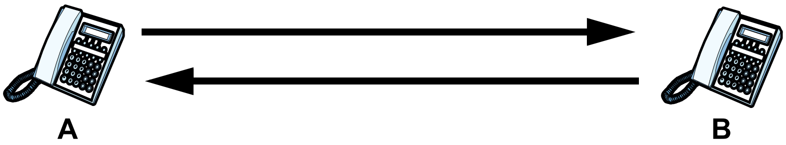
SIP Register Server

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

SIP User Agent

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

Figure 91 SIP User Agent



SIP Proxy Server

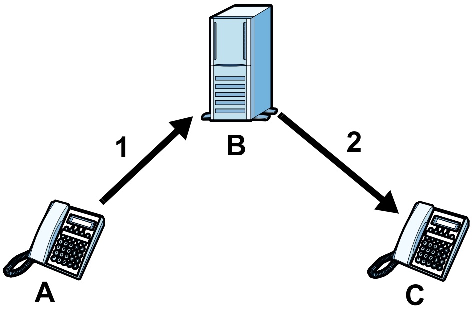
A SIP proxy server receives requests from clients and forwards them to another server.

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

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

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

Figure 92 SIP Proxy Server



STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the BM2022w to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the BM2022w to find the public IP address that NAT assigned, so the BM2022w can embed it in the SIP data stream. STUN does not work with symmetric NAT routers or firewalls. See RFC 3489 for details on STUN.

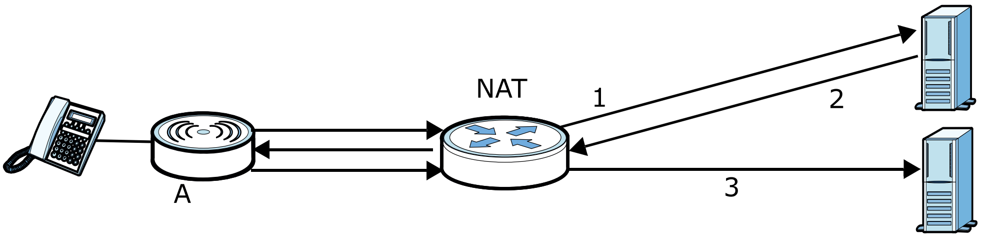
The following figure shows how STUN works.

1 The BM2022w (**A**) sends SIP packets to the STUN server (**B**).

2 The STUN server (**B**) finds the public IP address and port number that the NAT router used on the BM2022w's SIP packets and sends them to the BM2022w.

3 The BM2022w uses the public IP address and port number in the SIP packets that it sends to the SIP server (**C**).

Figure 93 STUN



Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the BM2022w's VoIP traffic. This allows the BM2022w to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the BM2022w to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).

NAT and SIP

The BM2022w must register its public IP address with a SIP register server. If there is a NAT router between the BM2022w and the SIP register server, the BM2022w probably has a private IP address. The BM2022w lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the BM2022w's IP address from inside the SIP message and maps it to your SIP identity. If the BM2022w has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity.

Use a SIP ALG (Application Layer Gateway), STUN, or outbound proxy to allow the BM2022w to list its public IP address in the SIP messages.

DTMF

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

Supplementary Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The BM2022w supports the following services:

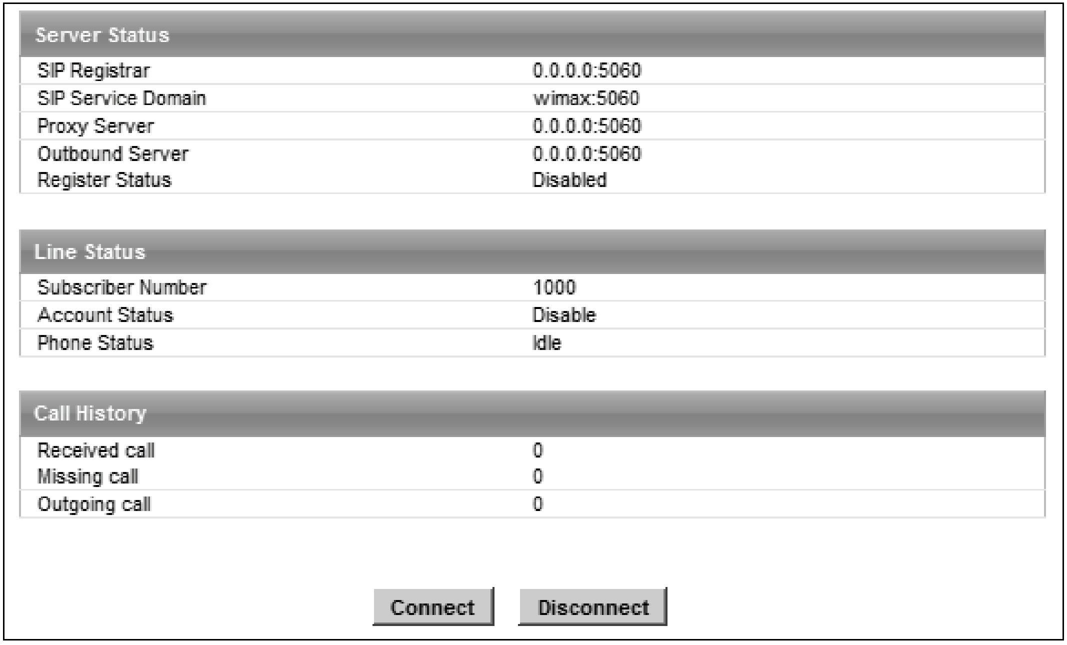
- Call Waiting
- Call Forwarding
- Caller ID

Note: To take full advantage of the supplementary phone services available though the BM2022w's phone port, you may need to subscribe to the services from your VoIP service provider.

10.2 Status

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

Figure 94 VoIP > Account 1 (or Account 2) > Status



Server Status

SIP Registrar	0.0.0.0:5060
SIP Service Domain	wimax:5060
Proxy Server	0.0.0.0:5060
Outbound Server	0.0.0.0:5060
Register Status	Disabled

Line Status

Subscriber Number	1000
Account Status	Disable
Phone Status	Idle

Call History

Received call	0
Missing call	0
Outgoing call	0

The following table describes the labels in this screen.

Table 72 VoIP > Account 1 (or Account 2) > Status

LABEL	DESCRIPTION
Server Status	
SIP Register	This field displays the IP address (or domain name) and service port number of the register server, if you have configured one.
SIP Service Domain	This field displays the SIP service domain and port number of the SIP server, if you have configured one.
Proxy Server	This field displays the IP address (or domain name) and service port number of the SIP proxy server, if you have configured one.

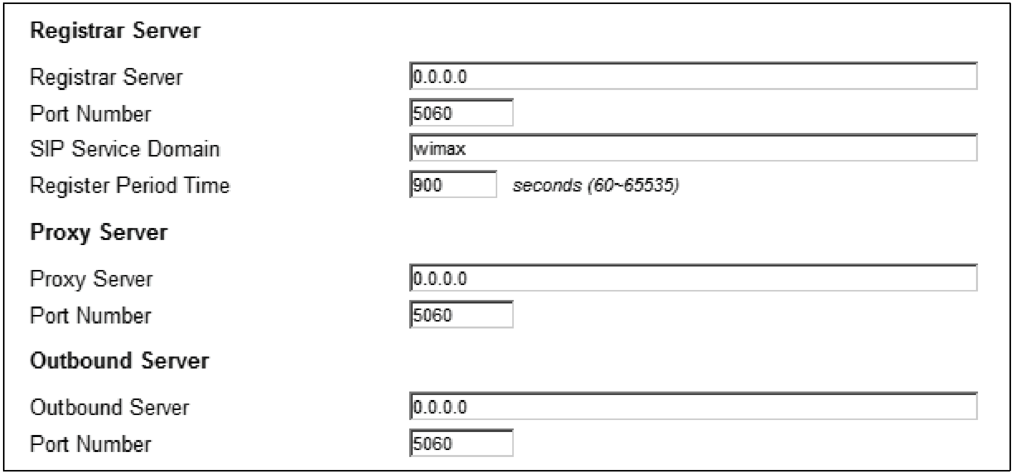
Table 72 VoIP > Account 1 (or Account 2) > Status

LABEL	DESCRIPTION
Outbound Server	This field displays the IP address (or domain name) and service port number of the outbound proxy server, if you have configured one.
Register Status	This field displays **Disabled** if the SIP account (set up in Section 10.4 on page 169) is disabled or de-registered from the registrar server. It displays **Registering** (or **Unregistering**) after sending out the SIP register (or unregister) message to make registration (or de-registration) at (or from) the SIP registrar server. If the registration fails, for example, rejected by SIP registrar server (due to wrong authentication data) or timeout to get response from the server, **Error** would be displayed. It displays **Up** if the SIP account is registered at the registrar server successfully.
Line Status	
Subscriber Number	This field displays the SIP phone number for the phone line.
Account Status	This indicates whether the SIP account is activated or not. **Enable** means activated and **Disable** means deactivated.
Phone Status	This field displays the phone status, such as **Idle**, **Calling**, **Ringing**, **Connecting**, **InCall**, **Hold**, and **Disconnecting**.
Call History	
Received call	This field displays the number of calls you have received through the connected phone since the BM2022w last restarted or was turned on.
Missing call	This field displays the number of calls you have missed since the BM2022w last restarted or was turned on.
Outgoing call	This field displays the number of calls you have made through the connected phone since the BM2022w last restarted or was turned on.
Connect	Click this to register the BM2022w to the specified register server.
Disconnect	Click this to de-register the BM2022w with the register server.

10.3 Server

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

Figure 95 VoIP > Account 1 (or Account 2) > Server



Registrar Server

Registrar Server: 0.0.0.0

Port Number: 5060

SIP Service Domain: wimax

Register Period Time: 900 seconds (60~65535)

Proxy Server

Proxy Server: 0.0.0.0

Port Number: 5060

Outbound Server

Outbound Server: 0.0.0.0

Port Number: 5060

The following table describes the labels in this screen.

Table 73 VoIP > Account 1 (or Account 2) > Server

LABEL	DESCRIPTION
Registrar Server	
Registrar Server	Enter the IP address or domain name of a register server. You can use up to 63 printable ASCII characters.
Port Number	Enter the SIP server's listening port number. Keep the default value, if you are not sure of this value.
SIP Service Domain	Enter the IP address or domain name of a SIP server, if your VoIP service provider gave you one. Otherwise, enter the same address that you have entered in the **Registrar Server** field. You can use up to 63 printable ASCII characters.
Register Period Time	Enter the registration expiry time in seconds for the SIP account specified in Section 10.4 on page 169. The allowable range is 60~65535 seconds. However, this value is just a default preference value by user, the actual registration expiry time used by the SIP account is determined by the registrar server after the registration process. Once the SIP account has registered at the registrar server successfully, the BM2022w will send a re-register message to keep alive the successfully registered status at every half of the registration expiry time determined by the registrar server. If the keep-alive action failed, the register status described in Section 10.2 on page 166 will become **Error** state and you can not make any call in this status. However, after 512 seconds (fixed value), the BM2022w will send a register message again to try to recover a successfully registered status.
Proxy Server	
Proxy Server	Enter the IP address or domain name of the SIP proxy server provided by your VoIP service provider. You can use up to 63 printable ASCII characters.

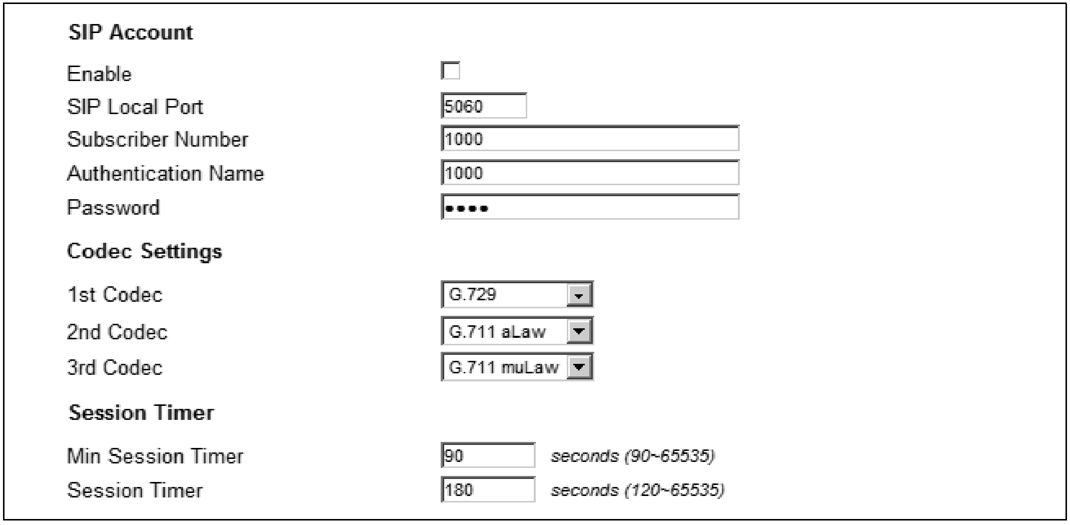
Table 73 VoIP > Account 1 (or Account 2) > Server

LABEL	DESCRIPTION
Port Number	Enter the SIP proxy server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Outbound Server	
Outbound Server	Enter the IP address or domain name of the outbound proxy server provided by your VoIP service provider. You can use up to 63 printable ASCII characters. If you choose not to use an outbound proxy server, set this to **0.0.0.0**.
Port Number	Enter the outbound proxy's listening port number, if your VoIP service provider gave you one. Otherwise, leave it as the default '5060'. If the outbound proxy is disabled (set to **0.0.0.0**), then this port will be ignored.

10.4 SIP

Click **VoIP > Account 1 (or Account 2) > SIP** to configure SIP settings.

Figure 96 VoIP > Account 1 (or Account 2) > SIP



SIP Account

Enable □

SIP Local Port 5060

Subscriber Number 1000

Authentication Name 1000

Password ●●●●

Codec Settings

1st Codec G.729

2nd Codec G.711 aLaw

3rd Codec G.711 muLaw

Session Timer

Min Session Timer 90 *seconds (90~65535)*

Session Timer 180 *seconds (120~65535)*

The following table describes the labels in this screen.

Table 74 VoIP > Account 1 (or Account 2) > SIP

LABEL	DESCRIPTION
SIP Account	
Enable	Select this if you want the BM2022w to use this account. Clear it if you do not want the BM2022w to use this account.
SIP Local Port	Enter the BM2022w's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Subscriber Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 1-31 printable ASCII characters.
Authentication Name	Type the SIP user name associated with this account for authentication to the SIP register server. This field can be 1-31 printable characters (A-Z, a-z, 0-9).

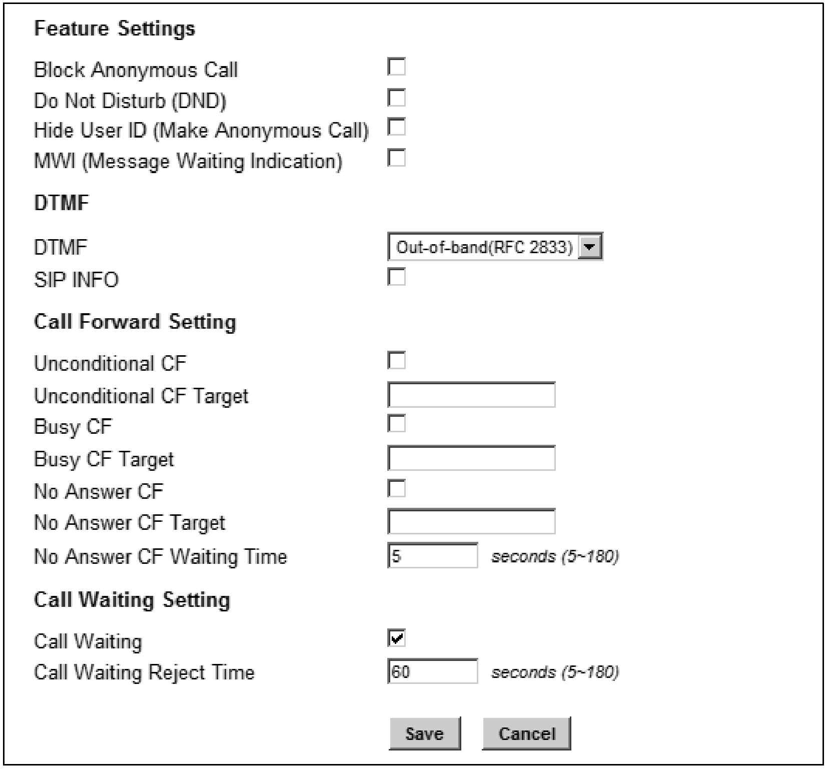
Table 74 VoIP > Account 1 (or Account 2) > SIP

LABEL	DESCRIPTION
Password	Type the SIP password associated with this account. This field can be 0-31 printable characters (A-Z, a-z, 0-9), underscores (_), pluses (+), periods (.), and "at" symbols (@).
Codec Settings	
1st Codec, 2nd Codec, 3rd Codec	Select the BM2022w's first, second, and third choices of the type of voice coder/decoder (codec) that you want the phone line to use when communicating with the SIP server. The following codecs (shown in highest quality to lowest quality order) are supported by the BM2022w: • **G.711 aLaw** (typically used in Europe) • **G.711 muLaw** (typically used in North America and Japan) • **G.729** You can also select **NONE** for the 2nd and 3rd codecs if your VoIP service provider only gave you one or two codec settings. When two SIP devices start a SIP session, they must agree on a codec.
Session Timer	
Min Session Timer	Enter the minimum session expiry time in seconds. The allowable range is 90~65535 seconds. When an incoming call requests a session expiry time that is lower than this value, the BM2022w will respond with a "423 session timer too small" message and tell the peer to use this value as the minimum bound.
Session Timer	Enter the session expiry time in seconds for all phone connections on this trunk. The allowable range is 120~65535 seconds. This value cannot be lower than the **Min Session Timer**. The BM2022w will use INVITE or UPDATE method to keep alive a session every half of the session expiry time during a call. If the keep-alive action is successful, the BM2022w will re-start the timer and do another keep-alive action after it reaches half of the session expiry time. If the keep-alive action failed, the call will terminate automatically. See Section 9.4 on page 161 to configure the Refresh Method with the INVITE or UPDATE method.

10.5 Feature

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

Figure 97 VoIP > Account 1 (or Account 2) > Feature



Feature Settings

Block Anonymous Call □
Do Not Disturb (DND) □
Hide User ID (Make Anonymous Call) □
MWI (Message Waiting Indication) □

DTMF

DTMF Out-of-band(RFC 2833)
SIP INFO □

Call Forward Setting

Unconditional CF □
Unconditional CF Target
Busy CF □
Busy CF Target
No Answer CF □
No Answer CF Target
No Answer CF Waiting Time 5 seconds (5~180)

Call Waiting Setting

Call Waiting ☑
Call Waiting Reject Time 60 seconds (5~180)

The following table describes the labels in this screen.

Table 75 VoIP > Account 1 (or Account 2) > Feature

LABEL	DESCRIPTION
Feature Settings	
Block Anonymous Call	Select this to have the BM2022w block all incoming calls from phone that do not send caller ID.
Do Not Disturb (DND)	Select this to have the BM2022w not forward calls to the phone line while processing incoming calls. Thus, for any incoming call, the remote peer can hear ringback tone, but the phone connected on the BM2022w would not ring. Meanwhile, the BM2022w can still make outgoing calls as usual. Note: The DND function should be used very carefully, since enabling DND makes the BM2022w not forward any incoming call to the phone line so the user would never know whether there are any incoming calls.
Hide User ID (Make Anonymous Call)	Select this to not have your Caller ID(number) displayed on the callee's screen.

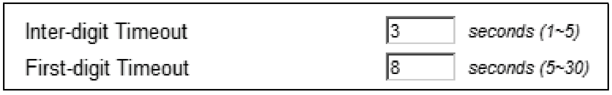
Table 75 VoIP > Account 1 (or Account 2) > Feature

LABEL	DESCRIPTION
MWI (Message Waiting Indication)	Select this to enable Message Waiting Indicator (MWI) function for this SIP account specified in Section 10.4 on page 169. When there is at least one new voicemail for the SIP account, the voice LED (described in Section 1.2.1 on page 19) turns yellow and the BM2022w sends a beeping tone to the phone while user picks-up the phone to make calls.
DTMF	
DTMF	Control how the BM2022 handles the DTMF tone relay to the communication peer. The DTMF tone is generated by the phone when you push its digit buttons during a call. One application is to send numbers when trying to do IVR (Interactive Voice Response) service with server. You should use the same mode as your VoIP service provider. The choices are: • **Out-of-band(RFC 2833)** - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • **In Band** - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones.
SIP INFO	Select this to have the BM2022w send the DTMF tones in SIP messages.
Call Forward Setting	
Unconditional CF, Unconditional CF Target	Select this if you want the BM2022w to forward all incoming calls to the specified phone number, regardless of other rules in this Call Forward Setting section. Specify the phone number in the **Unconditional CF Target** field. Note: The Unconditional CF function should be used very carefully, since enabling this function makes the BM2022w forward all incoming calls to another phone number, so the user would never know if there are any incoming calls.
Busy CF, Busy CF Target	Select this if you want the BM2022w to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **Busy CF Target** field. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer CF, No Answer CF Target, No Answer CF Waiting Time	Select this if you want the BM2022w to forward incoming calls to the specified phone number if the call is unanswered. Specify the phone number in the **No Answer CF Target** field on the right. Specify the time to wait before forwarding incoming calls in the **No Answer CF Waiting Time** field.
Call Waiting Setting	
Call Waiting	Select this to enable call waiting for this SIP account on the BM2022w.
Call Waiting Reject Time	Enter time to wait before rejecting a call when call waiting is enabled.

10.6 Dialing

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

Figure 98 VoIP > Account 1 (or Account 2) > Dialing



Inter-digit Timeout 3 seconds (1~5)

First-digit Timeout 8 seconds (5~30)

The following table describes the labels in this screen.

Table 76 VoIP > Account 1 (or Account 2) > Dialing

LABEL	DESCRIPTION
Inter-digit Timeout	Set the time in seconds (1~5) the BM2022w waits for each digit input of a complete callee number after you press the first key on the phone. If the BM2022w cannot receive the next digit entered within this time period, the BM2022w processes digits you have dialed.
First-digit Timeout	Set the number of seconds (5~30) for the BM2022w to wait for you to start dialing a number after you pick up the telephone receiver. If you do not dial any number within that time period, the dial tone becomes a busy signal. Put back the receiver and pick it up again if you want to make a new call.

10.7 FAX

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

Figure 99 VoIP > Account 1 (or Account 2) > FAX

Options: G.711 Pass Through

The following table describes the labels in this screen.

Table 77 VoIP > Account 1 (or Account 2) > FAX

LABEL	DESCRIPTION
Options	Select which standard the BM2022w uses to handle faxes. The peer devices must also use standard. **G.711A Pass Through** - Select this option to send and receive fax messages over the network or Internet using VoIP (G.711a). By encoding fax data as audio data, faxes may be susceptible to packet loss and other errors. However, as this standard is considerably older than T.38, it is more compatible with older obsolete systems. **T.38 FAX Relay** - BM2022w encodes fax messages to T.38 packets and sends as UDP packets through IP networks. This provides better quality, but it may have interoperability problems.

10.8 Technical Reference

The following section contains additional technical information about the BM2022w features described in this chapter.

10.8.1 SIP Call Progression with Session Timer

The following figure displays the basic steps in the setup and tear down of a SIP call with session timer supported by both peers. The UPDATE method is used to refresh the session. A calls B and uses proxy server P. Messages include Session Expiry (SE) and Minimum Session Expiry (MSE) time values. When the duration of the call reaches half of the SE time period, the session is refreshed.

Table 78 SIP Call Progression

A	P	B
1. INVITE SE: 60 ------------------>		
	2. 422 MSE: 3600 <-----------------------	
3. ACK ------------------>		
4. INVITE SE: 3600 MSE: 3600 ------------------>		
	5. INVITE SE: 3600 MSE: 3600 ------------------------>	
		6. INVITE SE: 3600 MSE: 3600 -------------------->
		7. OK SE: 3600 <--------------------
	8. OK SE: 3600 <------------------------	
9. OK SE: 3600 <------------------		
10. ACK ------------------>		
	11. ACK ------------------------>	-------------------->
	12. Dialogue (voice traffic)	

Table 78 SIP Call Progression (continued)

A	P	B
13. UPDATE SE: 3600 ------------------>		
	14. UPDATE SE:3600 ----------------------->	-------------------->
	<----------------------	15. OK SE: 3600 <-------------------
16. OK SE: 3600 <------------------		
17. BYE ------------------>		
		18. OK <-------------------

1 A sends a SIP INVITE request. This message is an invitation for B to participate in a SIP telephone call. A's INVITE specifies a SE of 60 seconds.

2 A's request arrives at P but is below the minimum allowed value of 3600, so it is rejected with a 422 message, which contains the MSE of 3600.

3 A sends an ACK to acknowledge the message was received.

4 A retries the INVITE request with SE of 3600 and MSE of 3600.

5 The SE in the new INVITE is acceptable so P forwards it to B.

6 B receives the INVITE.

7 B responds with an OK message which includes the SE of 3600.

8 P forwards the OK message to A.

9 A receives the OK.

10 A then sends an ACK message to acknowledge that the call is established completely.

11 The proxy server forwards the ACK message to B.

12 Now A and B exchange voice media (talk).

13 After around half of the SE time period is reached, or 1800 seconds in this case, A sends an UPDATE request to refresh the session.

14 The UPDATE request is forwarded by P to B.

15 B receives the UPDATE request and responds with an OK message.

16 The OK message is received by A.

17 After talking, A hangs up and sends a BYE request.

18 B replies with an OK response confirming receipt of the BYE request and the call is terminated.

10.8.2 SIP Client Server

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

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

For more information on the SIP protocol, please refer to RFC 3261.

11

The VoIP Line Screens

11.1 Overview

The **VoIP > Line** screens allow you to configure the volume, echo cancellation, VAD settings and custom tones for phone ports 1 and 2 which map to SIP accounts 1 and 2 (see Chapter 10 on page 163). Since both the **Line 1** and **Line 2** screens are quite similar, this section uses the **VoIP > Line 1** screens to describe the fields.

11.1.1 What You Can Do in This Chapter

- The **Phone** screen (Section 11.2 on page 178) lets you configure phone settings.
- The **Voice** screen (Section 11.3 on page 178) lets you configure voice settings.

11.1.2 What You Need to Know

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

Voice Activity Detection/Silence Suppression/Comfort Noise

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the BM2022w reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

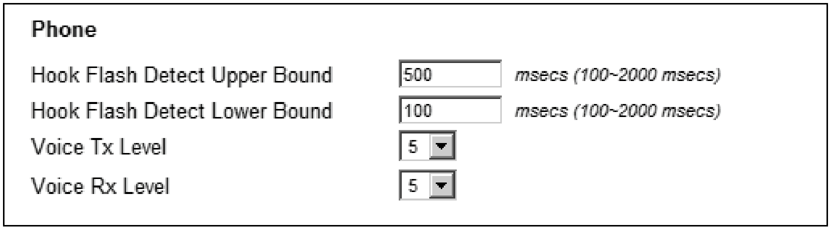
When using VAD, the BM2022w generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

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

11.2 Phone

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



Phone

Hook Flash Detect Upper Bound	500	msecs (100~2000 msecs)
Hook Flash Detect Lower Bound	100	msecs (100~2000 msecs)
Voice Tx Level	5 ▾	
Voice Rx Level	5 ▾	

Figure 100 VoIP > Line 1 (or Line 2) > Phone

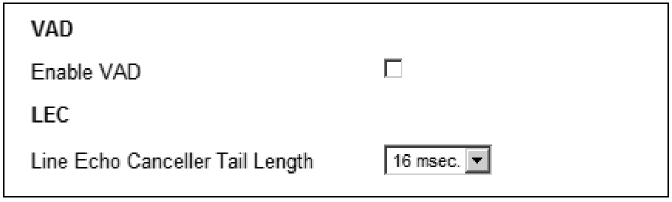
The following table describes the labels in this screen.

Table 79 VoIP > Line 1 (or Line 2) > Phone

LABEL	DESCRIPTION
Phone	
Hook Flash Detect Upper Bound	Enter the number of milliseconds for the upper bound of a quick on-hook and off-hook cycle in order to recognize a hook flash event.
Hook Flash Detect Lower Bound	Enter the number of milliseconds for the lower bound of a quick on-hook and off-hook cycle in order to recognize a hook flash event.
Voice Tx Level	Select the volume level transmitted by the BM2022w. -9 is the quietest, and 9 is the loudest.
Voice Rx Level	Select the volume level transmitted to the BM2022w. -9 is the quietest, and 9 is the loudest.

11.3 Voice

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



VAD

Enable VAD □

LEC

Line Echo Canceller Tail Length 16 msec. ▾

Figure 101 VoIP > Line 1 (or Line 2) > Voice

The following table describes the labels in this screen.

Table 80 VoIP > Line 1 (or Line 2) > Voice

LABEL	DESCRIPTION
VAD - Voice Activity Detection	
Enable VAD	Enable Voice Active Detector (VAD) to have the BM2022w stop transmitting voice traffic when you are not speaking using the detection method. This reduces the bandwidth the BM2022w uses.

Table 80 VoIP > Line 1 (or Line 2) > Voice

LABEL	DESCRIPTION
LEC - Line Echo Cancellation	
Line Echo Canceller Tail Length	Select the maximum number of milliseconds of an echo length (16 ms, 32 ms or 48 ms) the BM2022w can handle and eliminate the effect. An echo is normally caused by the sound of your voice reverberating in the telephone receiver while you talk. Select **Disable** to turn this feature off.

12

Maintenance

12.1 Overview

Use these screens to manage and maintain your BM2022w.

12.1.1 What You Need to Know

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

Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the BM2022w will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

Remote Management and NAT

When NAT is enabled:

- Use the BM2022w's WAN IP address when configuring from the WAN.
- Use the BM2022w's LAN IP address when configuring from the LAN.

System Timeout

There is a default system management idle timeout of five minutes. The BM2022w automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your BM2022w supports SNMP agent functionality, which allows a manager station to manage and monitor the BM2022w through the network. The BM2022w supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

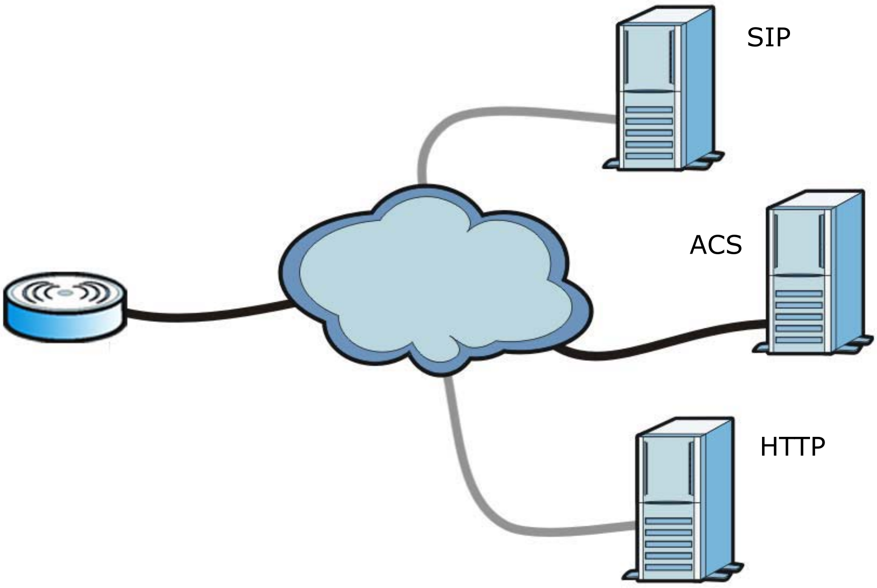
Note: SNMP is only available if TCP/IP is configured.

TR-069

TR-069 is an abbreviation of “Technical Reference 069”, a protocol designed to facilitate the remote management of Customer Premise Equipment (CPE), such as the BM2022w. It can be managed over a WAN by means of an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between the ACS and the client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the BM2022w, modify its settings, perform firmware upgrades, and monitor and diagnose it. In order to do so, you must enable the TR-069 feature on your BM2022w and then configure it appropriately. (The ACS server which it will use must also be configured by its administrator.)

Figure 103 TR-069 Example



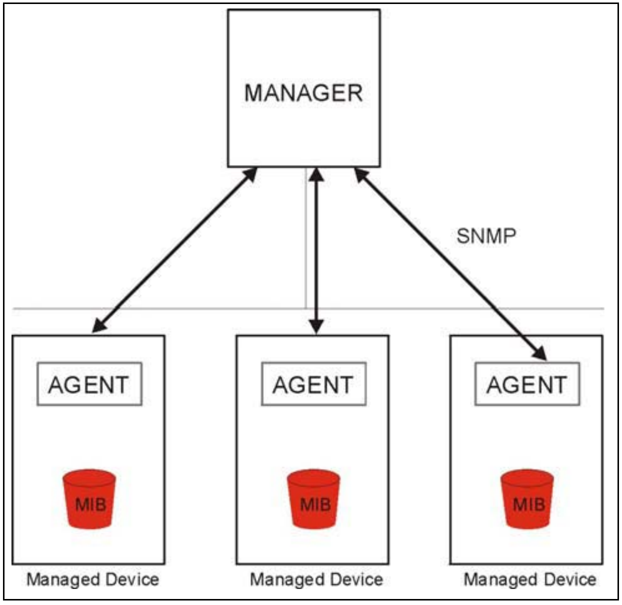
In this example, the BM2022w receives data from at least 3 sources: A SIP server for handling voice calls, an HTTP server for handling web services, and an ACS, for configuring the BM2022w remotely. All three servers are owned and operated by the client’s Internet Service Provider. However, without the configuration settings from the ACS, the BM2022w cannot access the other two servers. Once the BM2022w receives its configuration settings and implements them, it can connect to the other servers. If the settings change, it will once again be unable to connect until it receives its updates from the ACS.

The BM2022w can be configured to periodically check for updates from the auto-configuration server so that the end user need not be worried about it.

SNMP

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

Figure 104 SNMP Management Model



An agent is a management software module that resides in a managed device (the BM2022w). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects. The BM2022w supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

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

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

The BM2022w sends traps to the SNMP manager when any of the following events occurs:

Table 82 SNMP Traps

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

OMA-DM

When the BM2022w initiates communication with the server (often times at start up or after the first time you turn it on), the server uploads commands, new files (if any), and other information used by a service provider to customize the BM2022w’s features.

Device management works as follows:

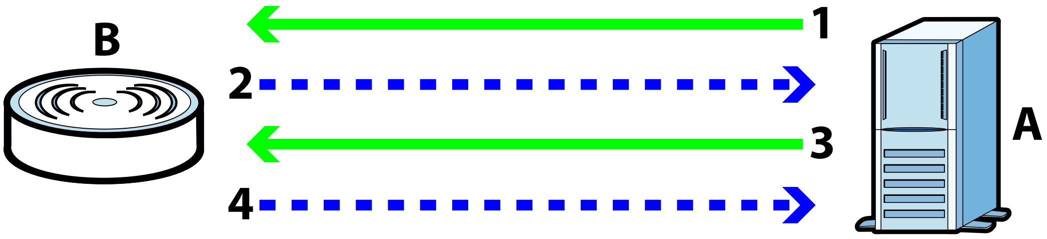
1 The server (**A**) sends out the query (**1**) to the BM2022w (**B**).

2 The BM2022w responds by sending back its credentials (**2**), to which the server responds with its credentials along with a string of management operations (**3**).

3 The client responds to the management operations (**4**), perhaps confirming file alterations or confirming receipt of file uploads and so on.

4 The server disconnects from the BM2022w once all of its management operations have been carried out.

Figure 105 OMA-DM Data Management



OMA-DM Authentication

In order to ensure the integrity of the connection between an OMA-DM server and the BM2022w, communication between the two is encoded using one of three common algorithms. They are not intended to be used in lieu of proper digital security, but instead as a means of transmitting multiple disparate types of data over HTTP. Security encryption for communication is handled by different processes configured elsewhere in the BM2022w's web configurator

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

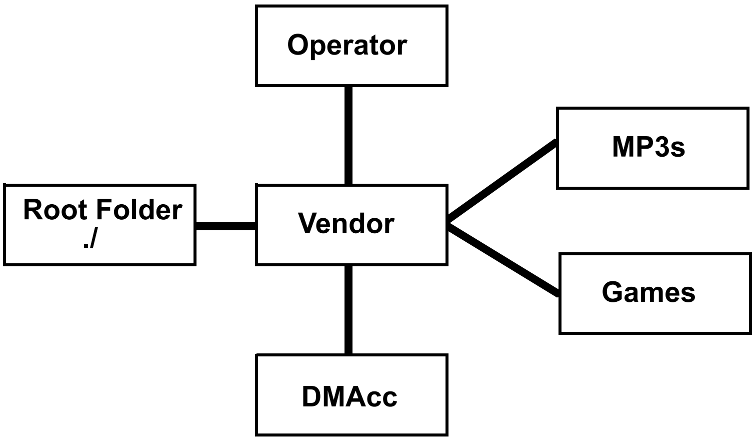
Digest Access Authentication – This protocol was designed to replace basic access authentication. Instead of encoding a user name and password in plaintext, this protocol uses what is known as an MD5 message authentication code. It allows the server to issue a single-use, randomly generated number (known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

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

OMA-DM Data Model

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

Figure 106 OMA-DM Data Model



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

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

Daytime

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

Time

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

NTP

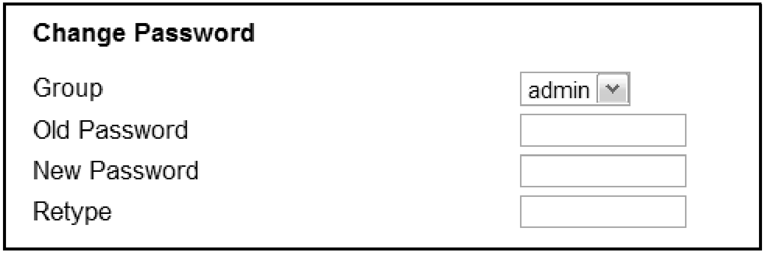
NTP stands for Network Time Protocol. It is employed by devices connected to the Internet in order to obtain a precise time setting from an official time server. These time servers are accurate to within 200 microseconds.

12.2 Password

Use this screen to set up admin and guest accounts for logging into and managing the WiMAX Device. The "admin" user can access and configure all screens. The "guest" user can only perform some basic settings such as viewing the system status information, configuring LAN, NAT, DDNS, and Firewall settings and reset the BM2022w to factory defaults and restart the BM2022w.

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

Figure 107 Password Screen



Change Password

Group: admin

Old Password

New Password

Retype

This screen contains the following fields:

Table 83 Password

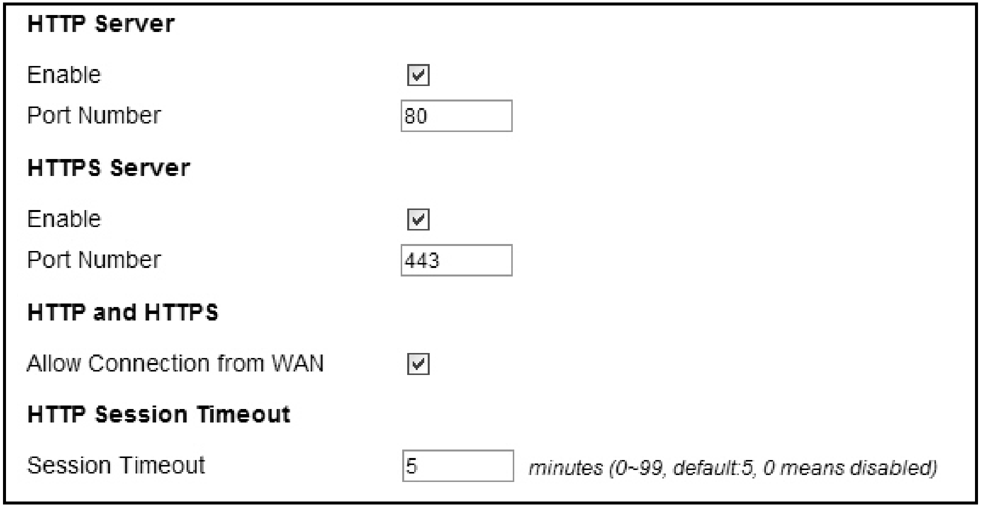
LABEL	DESCRIPTION
Group	Select the group for which you want to change the login password.
Old Password	Enter the old password for the login group.
New Password	Enter the new password for the login group.
Retype	Retype the new password for the login group.

12.3 HTTP

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

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

Figure 108 HTTP Screen



HTTP Server

Enable ☑

Port Number 80

HTTPS Server

Enable ☑

Port Number 443

HTTP and HTTPS

Allow Connection from WAN ☑

HTTP Session Timeout

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

This screen contains the following fields:

Table 84 HTTP

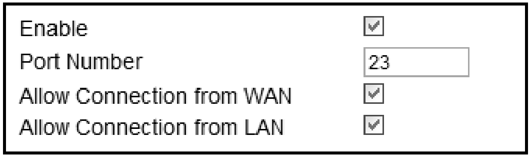
LABEL	DESCRIPTION
HTTP Server	
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the BM2022w. The computer must use the same port number.
HTTPS Server	
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the BM2022w. The computer must use the same port number.
HTTP and HTTPS	
Allow Connection from WAN	Select this to allow incoming connections from the WAN over either HTTP or HTTPS.
HTTP Session Timeout	
Session Timeout	Enter the number of minutes (0-99) the BM2022w waits to delete an inactive web connection (HTTP or HTTPS).

12.4 Telnet

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

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

Figure 109 Telnet Screen



Enable	☑
Port Number	23
Allow Connection from WAN	☑
Allow Connection from LAN	☑

This screen contains the following fields:

Table 85 Telnet

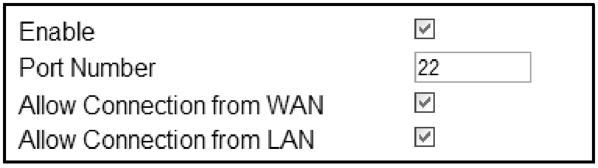
LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the BM2022w. The computer must use the same port number.
Allow Connection from WAN	Select this to allow connections using this service that originate on the WAN.
Allow Connection from LAN	Select this to allow connection using this service that originate on the LAN.

12.5 SSH

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

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

Figure 110 SSH Screen



Enable	☑
Port Number	22
Allow Connection from WAN	☑
Allow Connection from LAN	☑

This screen contains the following fields:

Table 86 SSH

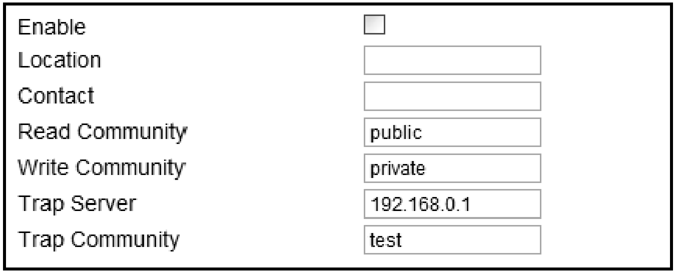
LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the BM2022w. The computer must use the same port number.
Allow Connection from WAN	Select this to allow connections using this service that originate on the WAN.
Allow Connection from LAN	Select this to allow connection using this service that originate on the LAN.

12.6 SNMP

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

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

Figure 111 SNMP Screen



Enable	□
Location	
Contact	
Read Community	public
Write Community	private
Trap Server	192.168.0.1
Trap Community	test

This screen contains the following fields:

Table 87 SNMP

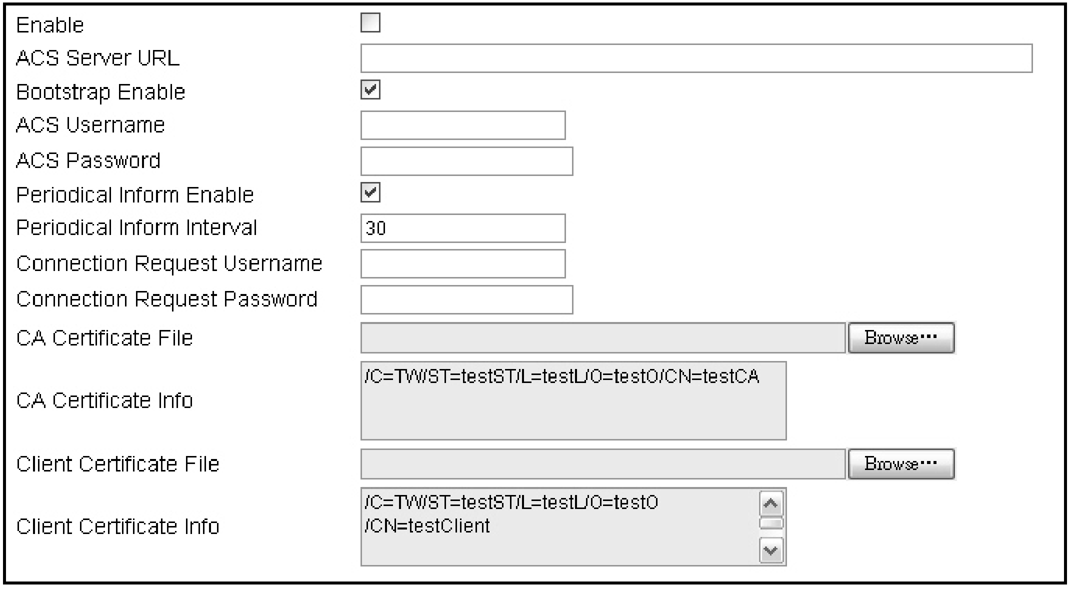
LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Location	Enter the location of the SNMP server (for example, "Engineering Dept., Floor 6, Building A, New York City").
Contact	Enter contact information for the administrator managing the SNMP server (for example, "Bill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

12.7 CWMP

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

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

Figure 112 CWMP Screen



Enable	□
ACS Server URL	
Bootstrap Enable	☑
ACS Username	
ACS Password	
Periodical Inform Enable	☑
Periodical Inform Interval	30
Connection Request Username	
Connection Request Password	
CA Certificate File	Browse...
CA Certificate Info	/C=TW/ST=testST/L=testL/O=testO/CN=testCA
Client Certificate File	Browse...
Client Certificate Info	/C=TW/ST=testST/L=testL/O=testO /CN=testClient

This screen contains the following fields:

Table 88 CWMP

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
ACS Server URL	Enter the URL or IP address of the auto-configuration server.
Bootstrap Enable	Select this to enable bootstrap events.
ACS Username	Enter the user name sent when the BM2022w connects to the ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.
ACS Password	Enter the password sent when the BM2022w connects to an ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.
Periodical Inform Enable	Select this to allow the BM2022w to periodically connect to the ACS and check for configuration updates. If you do not enable this feature then the BM2022w can only be updated automatically when the ACS initiates contact with it and if you selected the checkbox on this screen.
Periodical Inform Interval	Enter the time interval (in seconds) at which the BM2022w connects to the auto-configuration server.
Connection Request Username	Enter the connection request user name that the ACS must send to the BM2022w when it requests a connection. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed. Note: This must be provided by the ACS administrator.

Table 88 CWMP (continued)

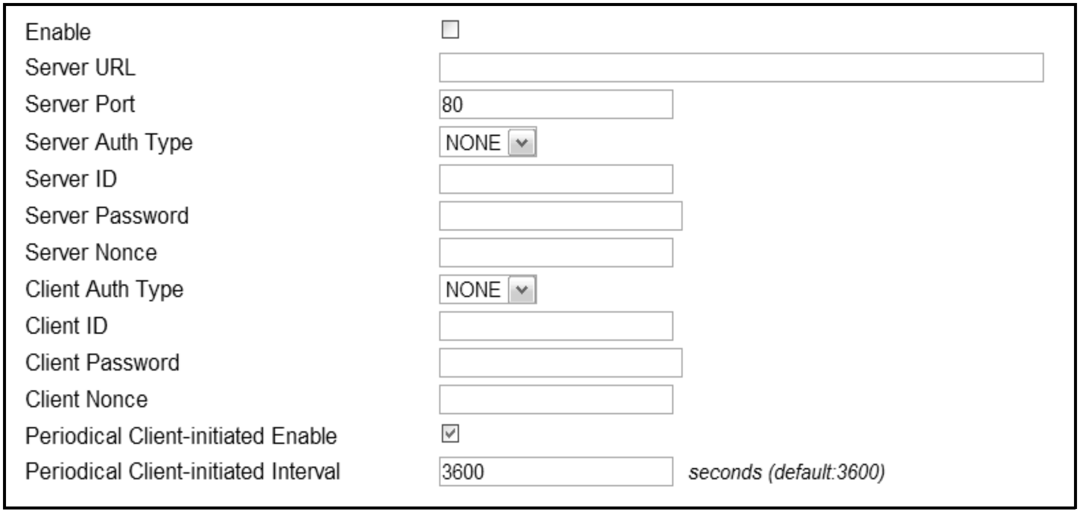
LABEL	DESCRIPTION
Connection Request Password	Enter the connection request password that the ACS must send to the BM2022w when it requests a connection. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed. Note: This must be provided by the ACS administrator.
CA Certificate File	Click **Browse** to upload a Certificate Authority (CA) certificate to the BM2022w.
CA Certificate Info	This displays information about the currently active CA certificate.
Client Certificate File	Click **Browse** to upload a client certificate to the BM2022w.
Client Certificate Info	This displays information about the currently active client certificate.

12.8 OMA-DM

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

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

Figure 113 OMA-DM Screen



Enable	☐
Server URL	
Server Port	80
Server Auth Type	NONE
Server ID	
Server Password	
Server Nonce	
Client Auth Type	NONE
Client ID	
Client Password	
Client Nonce	
Periodical Client-initiated Enable	☑
Periodical Client-initiated Interval	3600 *seconds (default:3600)*

This screen contains the following fields:

Table 89 OMA-DM

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Server URL	Enter the IP address or URL of the OMA-DM server that you intend to use to manage this device.
Server Port	Enter the port number for the IP address of the OMA-DM server set up in the preceding field.

Table 89 OMA-DM (continued)

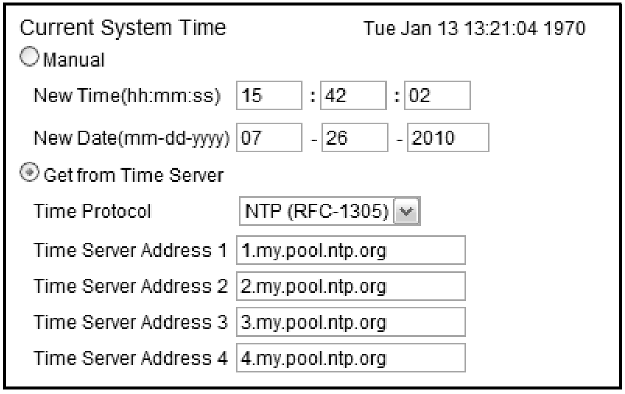
LABEL	DESCRIPTION
Server Auth Type	Select the encryption algorithm scheme used by the OMA-DM server to communicate with client devices. If the scheme selected here does not match the actual scheme used by the server, then server will challenge the BM2022w to automatically update its settings. • **None** - No authentication. • **Basic** - Server ID and Password are encoded using a Basic Access Authentication Code. • **Digest (MD5)** - Server ID and Password are encoded using a Digest Access Authentication Code. • **HMAC** - Server ID and Password are encoded using a keyed Hash Message Authentication Code.
Server ID	Enter the identification code for the server. This is used by the BM2022w during the communication handshake process to identify the server.
Server Password	Enter the password for the server's identification code. This shared public key is used by the BM2022w during the communication handshake process to identify the server.
Server Nonce	The BM2022w and the OMA-DM server use nonces to authenticate each other if you select **MD5** as the authentication algorithm in the **Server Auth Type** field. Nonce is an abbreviation of 'number used once'. It is normally a random or pseudo-random number applied in an authentication protocol to protect existing communications from being reused in 'replay attacks'. Type up to 20 digits for the OMA-DM server nonce.
Client Auth Type	Select the encryption algorithm scheme used by the OMA-DM server to communicate with client devices. If the scheme selected here does not match the actual scheme used by the server, then server will challenge the BM2022w to automatically update its settings. • **None** - No authentication. • **Basic** - Server ID and Password are encoded using a Basic Access Authentication Code. • **Digest (MD5)** - Server ID and Password are encoded using a Digest Access Authentication Code. • **HMAC** - Server ID and Password are encoded using a keyed Hash Message Authentication Code. Note: Make sure that the scheme selected here matches the **Server Auth Type**.
Client ID	Enter the client name for the BM2022w.
Client Password	Enter the password for the BM2022w's client name.
Client Nonce	The BM2022w and the OMA-DM server use nonces to authenticate each other if you select **MD5** as the authentication algorithm in the **Client Auth Type** field. Type up to 20 digits for the OMA-DM client nonce.
Periodical Client-Initiated Enable	Select this to allow the BM2022w to periodically connect to the OMA-DM server and check for configuration updates. If you do not enable this feature then the BM2022w can only be updated automatically when the OM-DM server initiates contact with it and if you selected the checkbox on this screen.
Periodical Client-Initiated Interval	Enter the time interval (in seconds) at which the BM2022w connects to the OMA-DM server.

12.9 Date

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

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

Figure 114 Date Screen



Current System Time Tue Jan 13 13:21:04 1970

○ Manual

New Time(hh:mm:ss) 15 : 42 : 02

New Date(mm-dd-yyyy) 07 - 26 - 2010

● Get from Time Server

Time Protocol NTP (RFC-1305)

Time Server Address 1 1.my.pool.ntp.org

Time Server Address 2 2.my.pool.ntp.org

Time Server Address 3 3.my.pool.ntp.org

Time Server Address 4 4.my.pool.ntp.org

This screen contains the following fields:

Table 90 Date

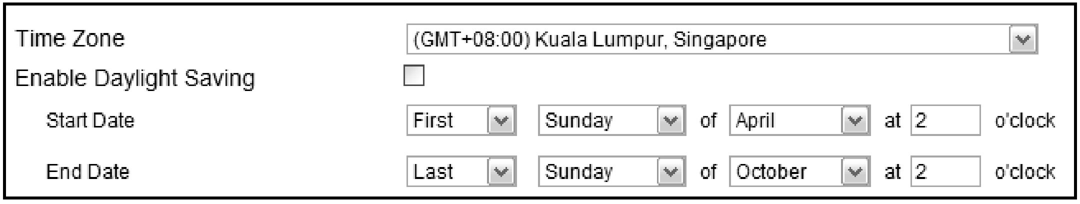
LABEL	DESCRIPTION
Manual	
New Time	Enter the new time in this field.
New Date	Enter the new date in this field.
Get from Time Server	
Time Protocol	Select the time service protocol that your time server uses.Check with your ISP or network administrator, or use trial-and-error to find a protocol that works. • **NTP (RFC 1305)** - This format is similar to Time (RFC 868).
Time Server Address 1~4	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.

12.10 Time Zone

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

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

Figure 115 Time Zone Screen



Time Zone (GMT+08:00) Kuala Lumpur, Singapore

Enable Daylight Saving □

Start Date First Sunday of April at 2 o'clock

End Date Last Sunday of October at 2 o'clock

This screen contains the following fields:

Table 91 Time Zone

LABEL	DESCRIPTION
Time Zone	Select the time zone at your location.
Enable Daylight Savings Time	Select this if your location uses daylight savings time. Daylight savings is a period from late spring to early fall when many places set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter which hour on which day of which week of which month daylight-savings time starts.
End Date	Enter which hour on the which day of which week of which month daylight-savings time ends.

12.11 Upgrade File

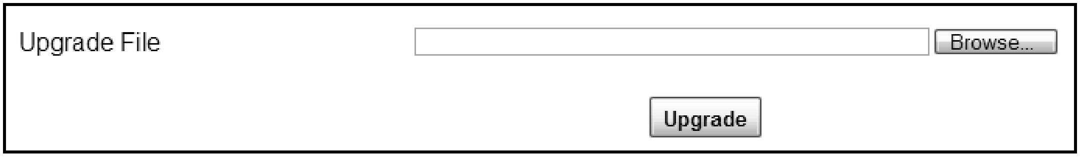
Use this screen to browse to a firmware file on a local computer and upload it to the WiMAX Device. Firmware files usually use the system model name with a "*.bin" extension, such as "BM2022w.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system restarts.

Contact your service provider for information on available firmware upgrades.

Note: Only use firmware for your BM2022w's specific model.

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

Figure 116 Upgrade File Screen



This screen contains the following fields:

Table 92 Upgrade File

LABEL	DESCRIPTION
Upgrade File	Click **Browse** then browse to the location of a firmware upgrade file and select it.
Upgrade	Click this to begin uploading the selected file. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress!

12.11.1 The Firmware Upload Process

When the BM2022w uploads new firmware, the process usually takes about two minutes. The device also automatically restarts in this time. This causes a temporary network disconnect.

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

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

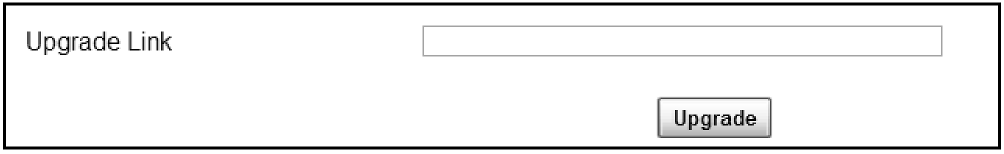
If the upload is not successful, you will be notified by error message.

12.12 Upgrade Link

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

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

Figure 117 Upgrade Link Screen



This screen contains the following fields:

Table 93 Upgrade Link

LABEL	DESCRIPTION
Upgrade Link	Enter the URL or IP address of the firmware's upgrade location on the network.
Upgrade	Click this to begin uploading the selected file. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress!

12.13 CWMP Upgrade

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

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

Figure 118 CWMP Upgrade Screen

This screen contains the following fields:

Table 94 CWMP Upgrade

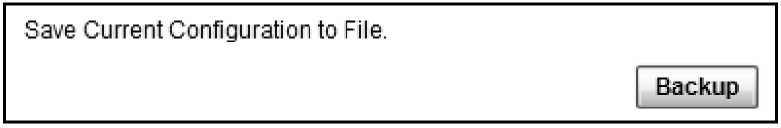
LABEL	DESCRIPTION
Upgrade	Click this to begin upgrading firmware using CWMP Request. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress!

12.14 Backup

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

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

Figure 119 Backup/Restore Screen


Save Current Configuration to File.

This screen contains the following fields:

Table 95 Backup/Restore

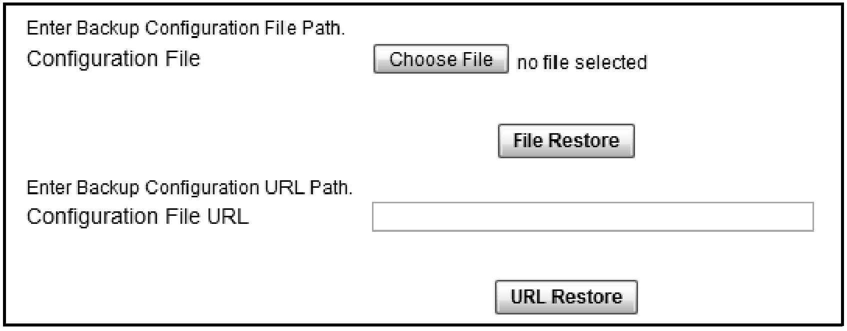
LABEL	DESCRIPTION
Backup	Click this to save the BM2022w's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.

12.15 Restore

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

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

Figure 120 Restore Screen


Enter Backup Configuration File Path.

Configuration File

Enter Backup Configuration URL Path.

Configuration File URL

This screen contains the following fields:

Table 96 Restore

LABEL	DESCRIPTION
Configuration File	Click **Choose File** then browse to the location of a firmware upgrade file and select it. Click **File Restore** to upload the specified configuration to the BM2022w and replace the current settings.
Backup Configuration File URL	Enter the URL or IP address of the backup configuration file's location on the network. Click **URL Restore** to upload the specified configuration to the BM2022w and replace the current settings.

12.15.1 The Restore Configuration Process

When the BM2022w restores a configuration file, the device automatically restarts. This causes a temporary network disconnect.

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

If the BM2022w's IP address is different in the configuration file you selected, you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See the Quick Start Guide or the appendices for details on how to set up your computer's IP address.

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

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

12.16 Factory Defaults

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

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

Figure 121 Factory Defaults Screen

Clear configuration and return to factory defaults.

This screen contains the following fields:

Table 97 Factory Defaults

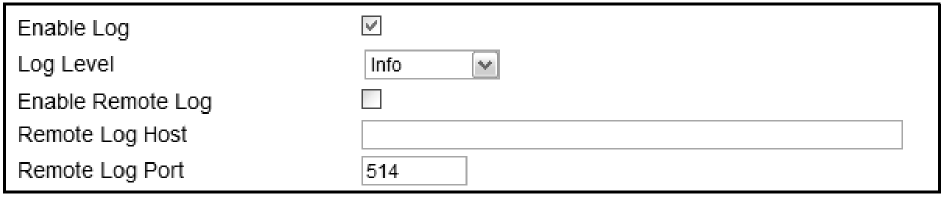
LABEL	DESCRIPTION
Reset	Click this to clear all user-entered configuration information and return the BM2022w to its factory defaults. There is no warning screen.

12.17 Log Setting

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

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

Figure 122 Log Setting Screen



Enable Log ☑

Log Level: Info

Enable Remote Log □

Remote Log Host

Remote Log Port: 514

This screen contains the following fields:

Table 98 Log Setting

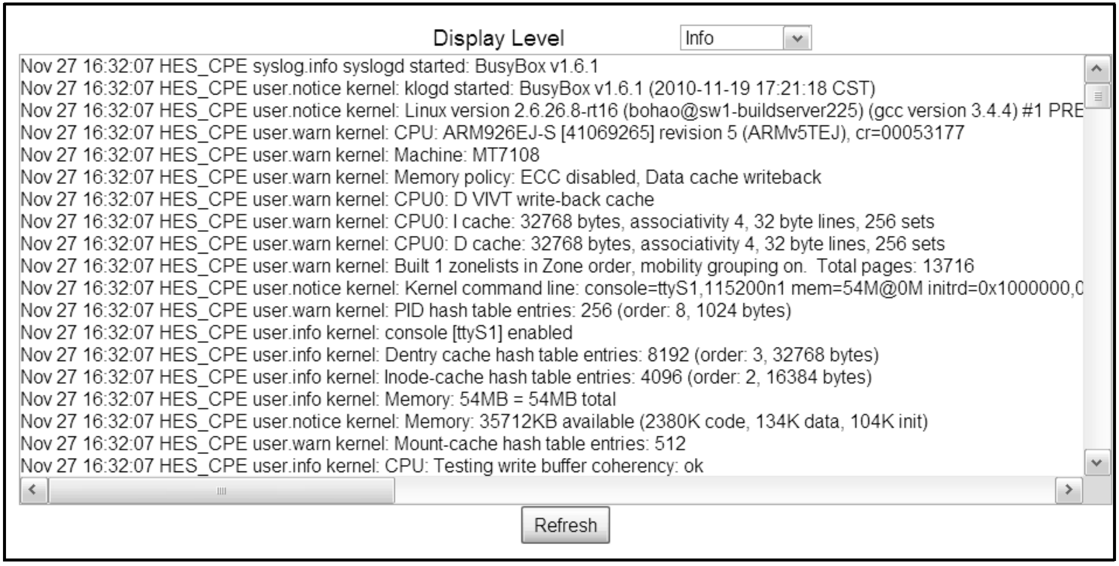
LABEL	DESCRIPTION
Enable Log	Select this to have the BM2022w log network activity according to the selected **Log Level**.
Log Level	Select the type of logs to record.
Enable Remote Log	Select this to allow logs to be recorded and stored on a remote logs server.
Remote Log Host	Enter the remote log host IP address if **Enable Remote Log** is selected.
Remote Log Port	Enter the remote log host port if **Enable Remote Log** is selected.

12.18 Log Display

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

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

Figure 123 Log Display Screen



Display Level: Info

```
Nov 27 16:32:07 HES_CPE syslog.info syslogd started: BusyBox v1.6.1
Nov 27 16:32:07 HES_CPE user.notice kernel: klogd started: BusyBox v1.6.1 (2010-11-19 17:21:18 CST)
Nov 27 16:32:07 HES_CPE user.notice kernel: Linux version 2.6.26.8-rt16 (bohao@sw1-buildserver225) (gcc version 3.4.4) #1 PRE
Nov 27 16:32:07 HES_CPE user.warn kernel: CPU: ARM926EJ-S [41069265] revision 5 (ARMv5TEJ), cr=00053177
Nov 27 16:32:07 HES_CPE user.warn kernel: Machine: MT7108
Nov 27 16:32:07 HES_CPE user.warn kernel: Memory policy: ECC disabled, Data cache writeback
Nov 27 16:32:07 HES_CPE user.warn kernel: CPU0: D VIVT write-back cache
Nov 27 16:32:07 HES_CPE user.warn kernel: CPU0: I cache: 32768 bytes, associativity 4, 32 byte lines, 256 sets
Nov 27 16:32:07 HES_CPE user.warn kernel: CPU0: D cache: 32768 bytes, associativity 4, 32 byte lines, 256 sets
Nov 27 16:32:07 HES_CPE user.warn kernel: Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 13716
Nov 27 16:32:07 HES_CPE user.notice kernel: Kernel command line: console=ttyS1,115200n1 mem=54M@0M initrd=0x1000000,0
Nov 27 16:32:07 HES_CPE user.warn kernel: PID hash table entries: 256 (order: 8, 1024 bytes)
Nov 27 16:32:07 HES_CPE user.info kernel: console [ttyS1] enabled
Nov 27 16:32:07 HES_CPE user.info kernel: Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
Nov 27 16:32:07 HES_CPE user.info kernel: Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
Nov 27 16:32:07 HES_CPE user.info kernel: Memory: 54MB = 54MB total
Nov 27 16:32:07 HES_CPE user.notice kernel: Memory: 35712KB available (2380K code, 134K data, 104K init)
Nov 27 16:32:07 HES_CPE user.warn kernel: Mount-cache hash table entries: 512
Nov 27 16:32:07 HES_CPE user.info kernel: CPU: Testing write buffer coherency: ok
```

This screen contains the following fields:

Table 99 Log Display

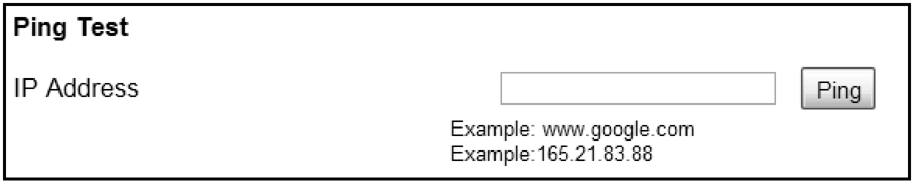
LABEL	DESCRIPTION
Display Level	Select the type of logs to display from this menu.
Refresh	Click this to refresh the logs in the display window.

12.19 Ping Test

Use this screen to test network connectivity using ping.

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

Figure 124 Ping Screen



Ping Test

IP Address

Example: www.google.com
Example:165.21.83.88

This screen contains the following fields:

Table 100 Ping

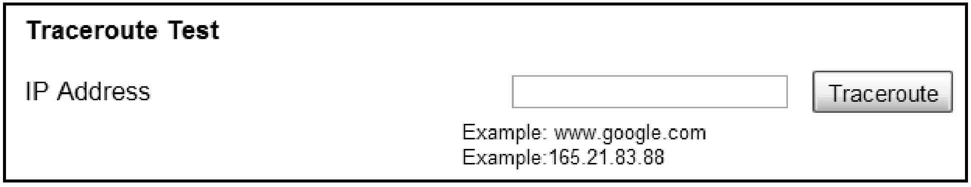
LABEL	DESCRIPTION
IP Address	Enter the IP address or domain name of a target device to which this test will send.
Ping	Click this to start the test. The result will show at the bottom of the screen.

12.20 Traceroute Test

Use this screen to test network connectivity using traceroute.

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

Figure 125 Traceroute Screen



Traceroute Test

IP Address

Example: www.google.com
Example:165.21.83.88

This screen contains the following fields:

Table 101 Traceroute

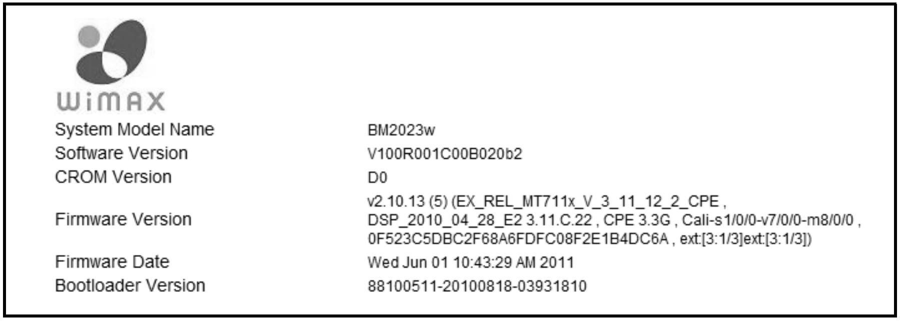
LABEL	DESCRIPTION
IP Address	Enter the IP address or domain name of a target device to which this test will send.
Traceroute	Click this to start the test. The result will show at the bottom of the screen.

12.21 About

This screen displays information about the BM2022w that can be useful when upgrading firmware, considering deployment options, and working with technical support if the device encounters difficulties.

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

Figure 126 About Screen



System Model Name	BM2023w
Software Version	V100R001C00B020b2
CROM Version	D0
Firmware Version	v2.10.13 (5) (EX_REL_MT711x_V_3_11_12_2_CPE , DSP_2010_04_28_E2 3.11.C.22 , CPE 3.3G , Cali-s1/0/0-v7/0/0-m8/0/0 , 0F523C5DBC2F68A6FDFC08F2E1B4DC6A , ext:[3:1/3]ext:[3:1/3])
Firmware Date	Wed Jun 01 10:43:29 AM 2011
Bootloader Version	88100511-20100818-03931810

This screen contains the following fields:

Table 102 About

LABEL	DESCRIPTION
System Model Name	This field displays the BM2022w system name. It is used for identification.
Software Version	This field displays the Web Configurator software version that the BM2022w is currently running.

Table 102 About (continued)

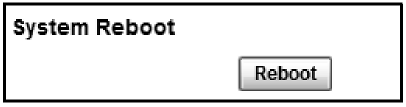
LABEL	DESCRIPTION
CROM Version	This field displays the CROM version number.
Firmware Version	This field displays the current version of the firmware inside the device.
Firmware Date	This field displays the date the firmware version was created.
Bootloader Version	This field displays the bootloader version.

12.22 Reboot

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

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

Figure 127 Reboot Screen



This screen contains the following fields:

Table 103 Reboot

LABEL	DESCRIPTION
Reboot	Click this button to have the device perform a software restart. The **Power** LED blinks as it restarts and the shines steadily if the restart is successful. Note: Wait one minute before logging back into the BM2022w after a restart.

13

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
- BM2022w Access and Login
- Internet Access
- Reset the BM2022w to Its Factory Defaults

13.1 Power, Hardware Connections, and LEDs

The BM2022w does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adapter or cord included with the BM2022w.
2. Make sure the power adapter or cord is connected to the BM2022w 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 BM2022w.
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 19 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 BM2022w.
5. If the problem continues, contact the vendor.

13.2 BM2022w Access and Login

I forgot the IP address for the BM2022w.

1 The default IP address is http://192.168.1.1**192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the BM2022w 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 BM2022w (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 BM2022w to its factory defaults. See Section 12.16 on page 197.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the BM2022w to its factory defaults. See Section 12.16 on page 197.

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 **192.168.1.1**http://192.168.1.1.
- If you changed the IP address (Section 7.6 on page 102), 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 BM2022w.

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 19.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix C on page 243.

4 If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. Your BM2022w 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 BM2022w. See Appendix D on page 253.

5 Reset the BM2022w to its factory defaults, and try to access the BM2022w with the default IP address. See Chapter 2 on page 21.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the BM2022w using another service, such as Telnet. If you can access the BM2022w, check the remote management settings and firewall rules to find out why the BM2022w 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 BM2022w.

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 BM2022w. Log out of the BM2022w 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 BM2022w.

4 If this does not work, you have to reset the BM2022w to its factory defaults. See Section 12.16 on page 197.

I cannot Telnet to the BM2022w.

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

13.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.2.1 on page 19.

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

3 Check your security settings. See Chapter 8 on page 129.

4 Check your WiMAX settings. The BM2022w may have been set to search the wrong frequencies for a wireless connection. See Chapter 6 on page 69. If you are unsure of the correct values, contact your service provider.

5 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

6 Disconnect all the cables from your BM2022w, 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 BM2022w), 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 19.

2 Disconnect and re-connect the power adapter to the BM2022w.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 The quality of the BM2022w's wireless connection to the base station may be poor. Poor signal reception may be improved by moving the BM2022w 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 BM2022w away or switch the other devices off. Weather conditions may also affect signal quality.

3 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.2.1 on page 19. If the BM2022w is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

4 Disconnect and re-connect the power adapter to the BM2022w.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

The Internet connection disconnects.

1 Check your WiMAX link and signal strength using the **Strength Indicator** LEDs on the device.

2 Contact your ISP if the problem persists.

13.4 Reset the BM2022w to Its Factory Defaults

If you reset the BM2022w, you lose all of the changes you have made. The BM2022w 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 BM2022w,

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 BM2022w restarts automatically, wait for the BM2022w to finish restarting, and log in to the web configurator. The password is "1234".

If the BM2022w does not restart automatically, disconnect and reconnect the BM2022w's power. Then, follow the directions above again.

13.4.1 Pop-up Windows, JavaScript and Java Permissions

Please see Appendix C on page 243.

14

Product Specifications

This chapter gives details about your BM2022w's hardware and firmware features.

Table 104 Environmental and Hardware Specifications

FEATURE	DESCRIPTION
Operating Temperature	0°C to 45°C
Storage Temperature	-25°C to 55°C
Operating Humidity	10% ~ 95% (non-condensing)
Storage Humidity	10% to 95% (non-condensing)
Power Supply	12V DC, 2A
Power consumption	Less than 20W
Ethernet Interface	Two auto-negotiating, auto-MDI/MDI-X NWay 10/100 Mbps RJ-45 Ethernet ports
Telephony Interface	Two analog ATA interfaces for standard telephones through RJ-11 FXS (Foreign Exchange Subscriber) analog connector
Antennas	Two 7 +/- 0.5dBi Omni directional antennas
Weight	600 g
Dimensions	165 mm (W) x 25 mm (D) x 260 mm (H)
Certification	• FCC • Comply with WiMAX Forum Wave II standard. • WEEE Eco directive 2002/95/EC. Full RoHS (6/6) • 2002/96/EC (WEEE) (WEEE) Waste Electrical and Electronic Equipment Directive • EEE (Proposal for Directive on Environmental Impacts of Electrical and Electronic Equipment). • Reach Compliance • EMC o EN 301 489-1 and EN 301 489-17. Emission class B. • RF ETSI o EN 302 326 • Safety o IEC 60950-1 and EN 60950-1.

Table 105 Radio Specifications

FEATURE	DESCRIPTION
Media Access Protocol	IEEE 802.16e
WiMAX Bandwidth	2.5 GHz
Data Rate	Aggregate throughput: up to 20 mbps Upload: 7 mbps
Modulation	QPSK (uplink and downlink) 16-QAM (uplink and downlink) 64-QAM (downlink only)

Table 105 Radio Specifications (continued)

Output Power	Typically 26.5 dBm with internal antennas
Duplex mode	Time Division Duplex (TDD)
Security	PKMv2 EAP-TTLS/CHAP/PAP/MSCHAP/MSCHAPv2 CMAC message authentication CCM mode 128-bit AES data ciphering Device authentication WiMAX Forum X.509 certificates

Table 106 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 BM2022w. You must connect using a compatible web browser in order to use it.
High Speed Wireless Internet Access	The BM2022w 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 BM2022w is a WiMAX mobile station (MS) compatible with the IEEE 802.16e standard.
Firewall	The BM2022w 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 BM2022w’s firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	The BM2022w can block access to web sites containing specified keywords. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering.
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
Universal Plug and Play (UPnP)	Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.
Dynamic DNS Support	With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.
DHCP	DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Your device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
Multiple SIP Accounts	You can configure multiple voice (SIP) accounts.

Table 106 Firmware Specifications (continued)

FEATURE	DESCRIPTION
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 BM2022w. You can also set the time manually.
Logging	Use the BM2022w's logging feature to view connection history, surveillance logs, and error messages.
Codecs	G.711 (PCM ì-law and a-law), G729, G.729a
Fax Support	T.38 FAX relay (FAX over UDP). G.711 fax relay for fax calls and be able to renegotiate codec to G.711 if a fax call is detected.
Ring Tones	Supports different distinctive ring tones on each line.
Call Prioritization	Prioritize VoIP traffic originating from the RJ-11 ports over any other traffic.

Table 107 Standards Supported

STANDARD	DESCRIPTION
RFC 768	User Datagram Protocol
RFC 791	Internet Protocol v4
RFC 792	Internet Control Message Protocol
RFC 792	Transmission Control Protocol
RFC 826	Address Resolution Protocol
RFC 854	Telnet Protocol
RFC 1112	IGMPv2
RFC 1349	Type of Service Protocol
RFC 1706	DNS NSAP Resource Records
RFC 1889	Real-time Transport Protocol (RTP)
RFC 1890	Real-time Transport Control Protocol (RTCP)
RFC 2030	Simple Network Time Protocol
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2236	IGMPv2
RFC 2131	Dynamic Host Configuration Protocol
RFC 2401	Security Architecture for the Internet Protocol
RFC 2409	Internet Key Exchange
RFC 2475	Architecture for Differentiated Services (Diffserv)

Table 107 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 2543	SIP Protocol
RFC 2617	Hypertext Transfer Protocol (HTTP) Authentication: Basic and Digest Access Authentication
RFC 2782	A DNS RR for specifying the location of services (DNS SRV)
RFC 2833	Real-time Transport Protocol Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2976	The SIP INFO Method
RFC 3261	Session Initiation Protocol (SIP version 2)
RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP).
RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3323	A Privacy Mechanism for SIP
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3489	NAT Traversal - STUN
RFC 3550	RTP - A Real Time Protocol for Real-Time Applications
RFC 3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)-XR
RFC 3715	IP Sec/NAT Compatibility
RFC 3842	A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
IEEE 802.3	10BASE5 10 Mbit/s (1.25 MB/s)
IEEE 802.3u	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) with auto-negotiation

Table 108 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 BM2022w 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 BM2022w 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 BM2022w 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 BM2022w wait a specified length of time before dialing the number.

Table 108 Voice Features

Phone config	The phone configuration table allows you to customize the phone keypad combinations you use to access certain features on the BM2022w, such as call waiting, call return, call forward, etc. The phone configuration table is configurable in command interpreter mode.
Firmware update enable / disable	If your service provider uses this feature, you hear a recorded message when you pick up the phone when new firmware is available for your BM2022w. Enter *99# in your phone's keypad to have the BM2022w 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 BM2022w 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 BM2022w 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 109 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

Table 109 Star (*) and Pound (#) Code Support

*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 BM2022w'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.

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 BM2022w 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 Huawei 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.

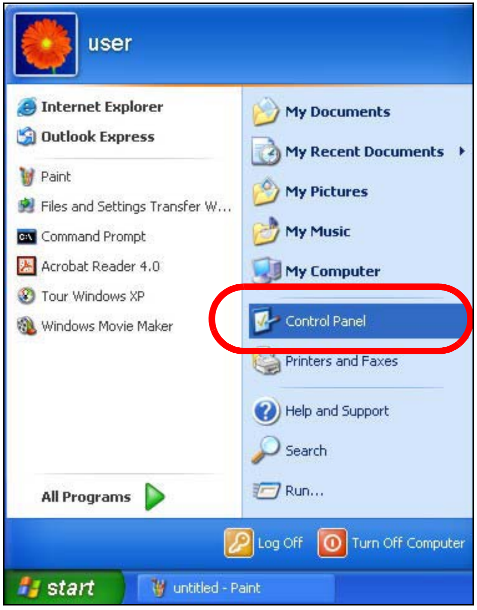
In this appendix, you can set up an IP address for:

Windows XP/NT/2000

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

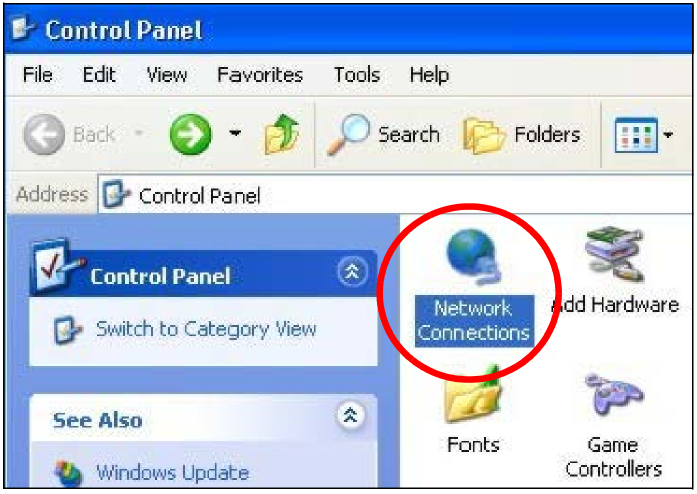
1 Click **Start** > **Control Panel**.

Figure 128 Windows XP: Start Menu



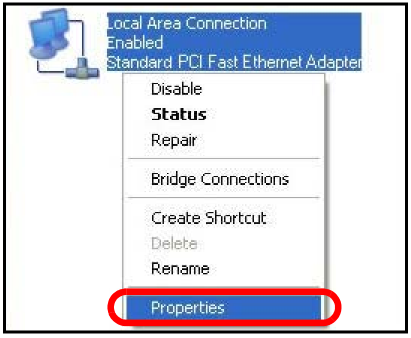
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 129 Windows XP: Control Panel



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

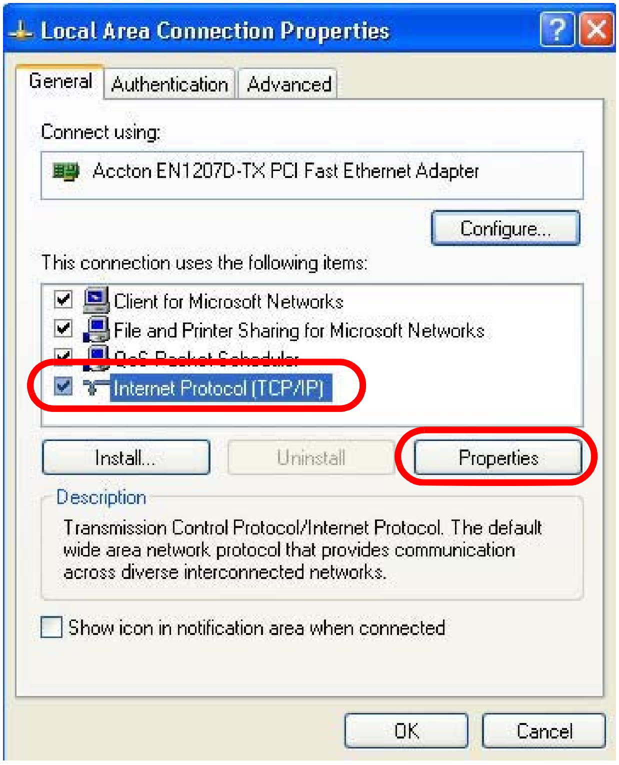
Figure 130 Windows XP: Control Panel > Network Connections > Properties



Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter

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

Figure 131 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)

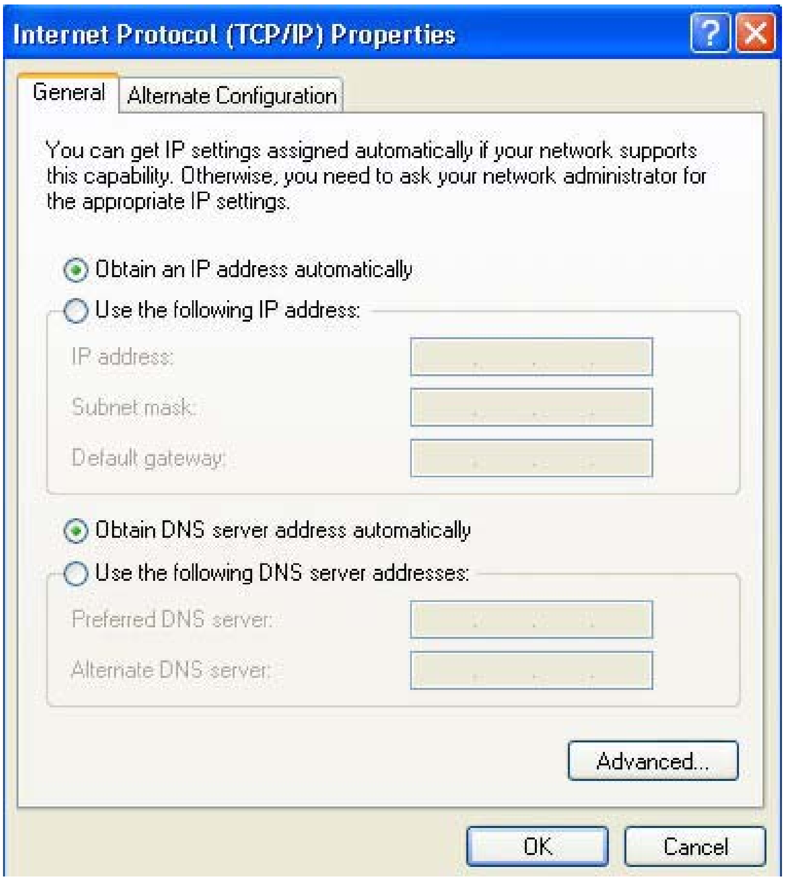
Description

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 132 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:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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].

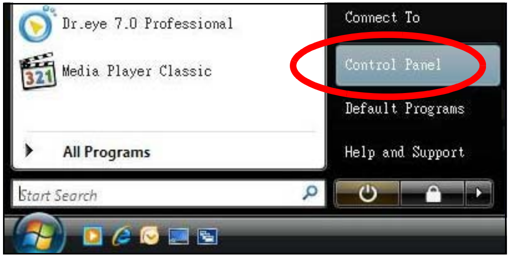
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

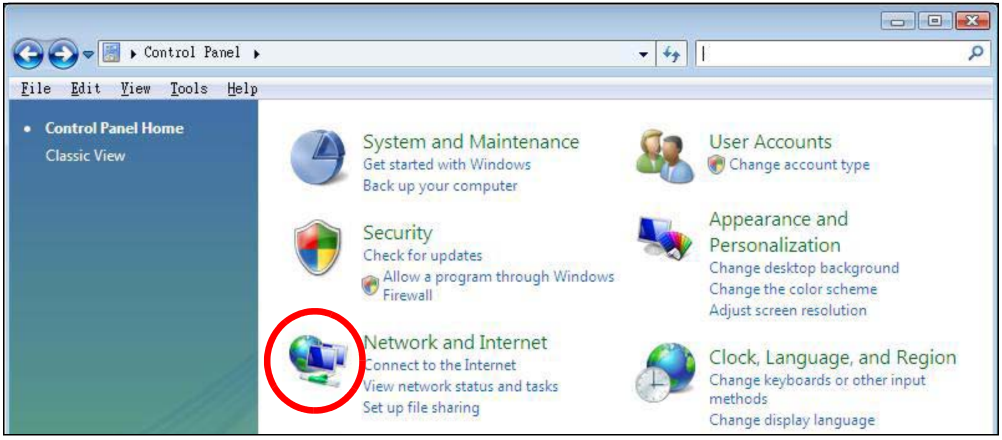
1 Click **Start** > **Control Panel**.

Figure 133 Windows Vista: Start Menu



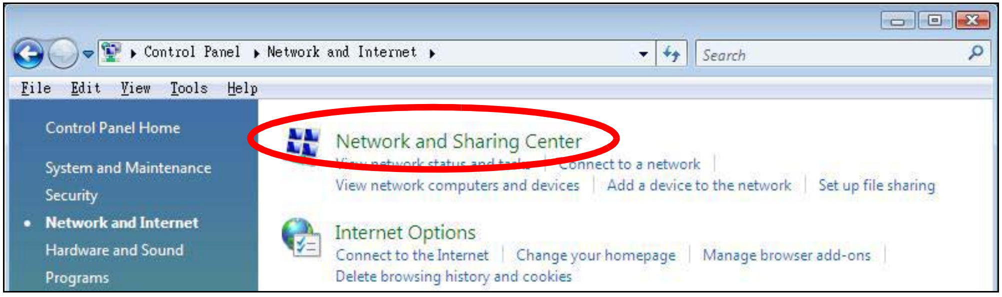
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 134 Windows Vista: Control Panel



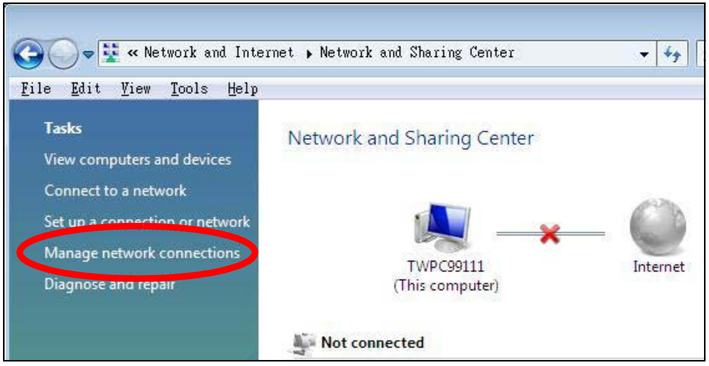
3 Click the **Network and Sharing Center** icon.

Figure 135 Windows Vista: Network And Internet



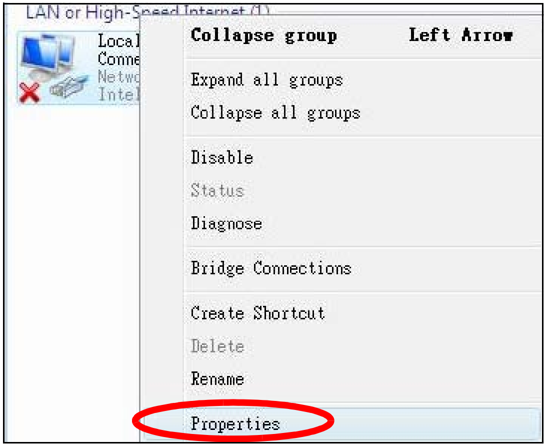
4 Click **Manage network connections**.

Figure 136 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**.

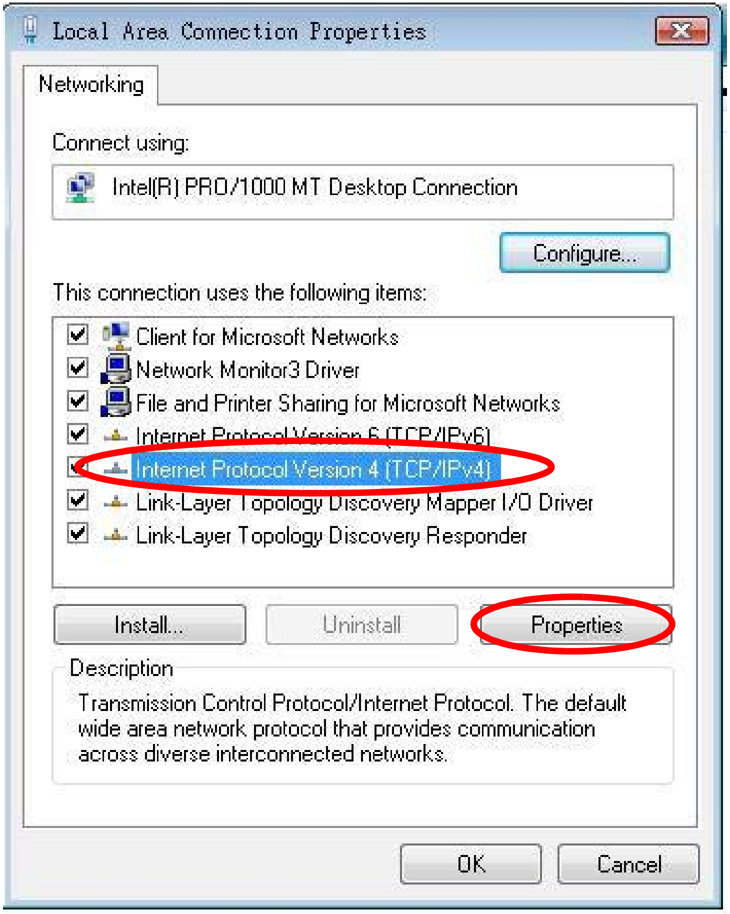
Figure 137 Windows Vista: Network and Sharing Center



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 138 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

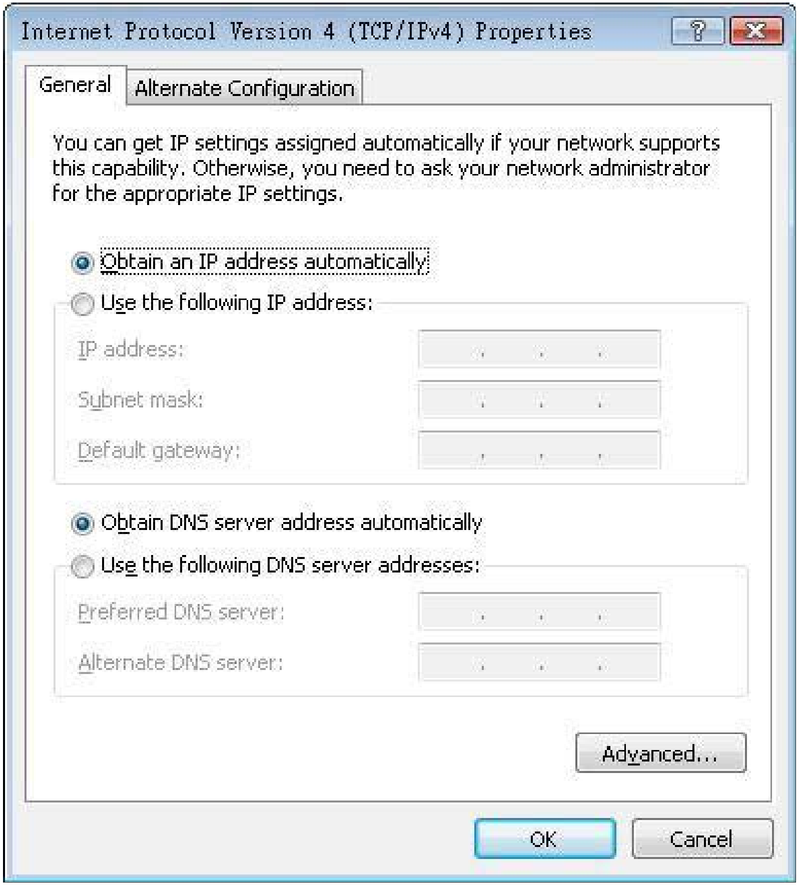
Description

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



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].

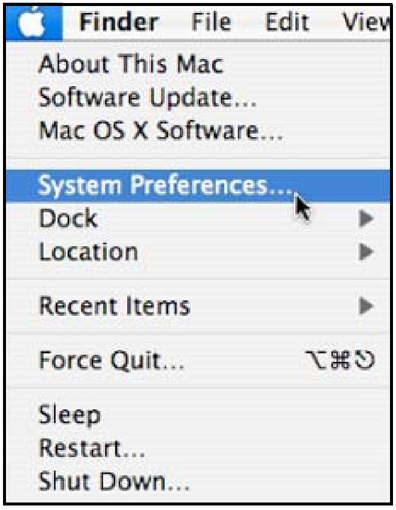
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

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.

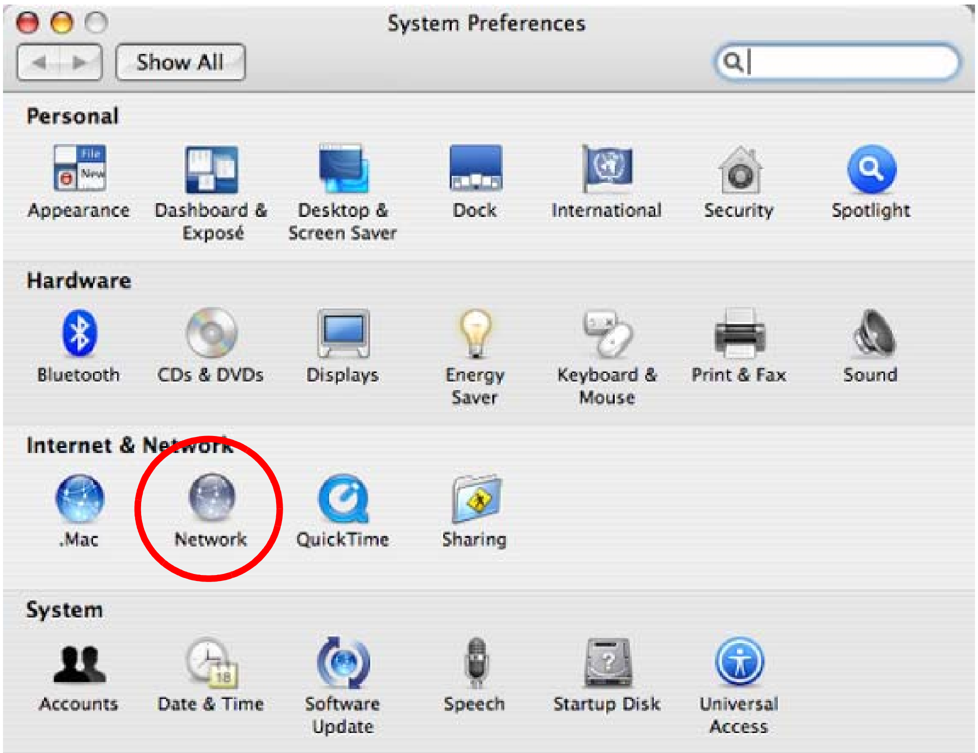
1 Click **Apple** > **System Preferences**.

Figure 140 Mac OS X 10.4: Apple Menu



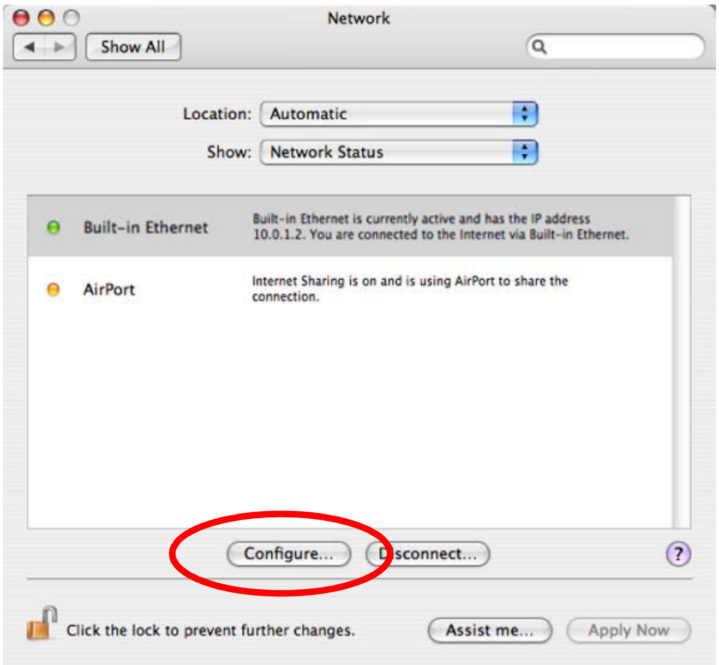
2 In the **System Preferences** window, click the **Network** icon.

Figure 141 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 142 Mac OS X 10.4: Network Preferences



Location: Automatic

Show: Network Status

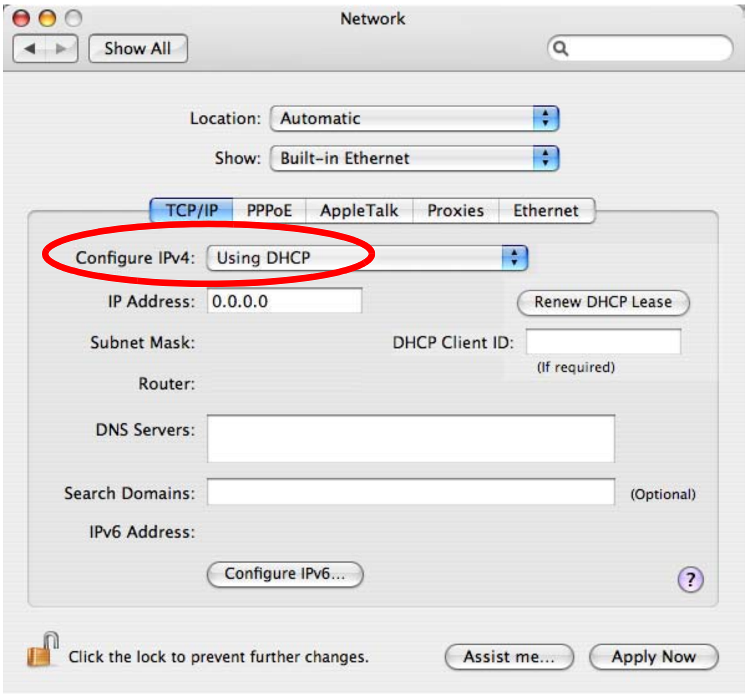
Built-in Ethernet — Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.

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

Click the lock to prevent further changes.

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

Figure 143 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)

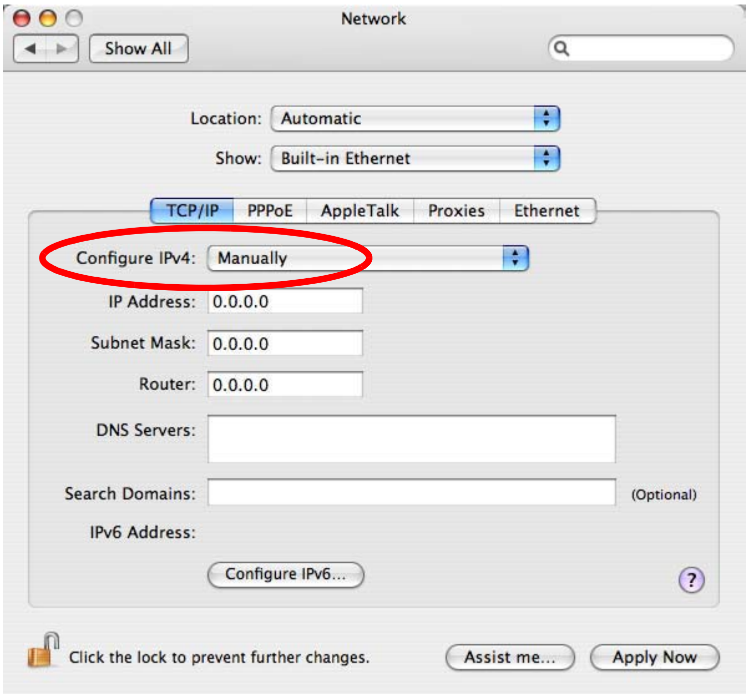
IPv6 Address:

Click the lock to prevent further changes.

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 144 Mac OS X 10.4: Network Preferences > Ethernet

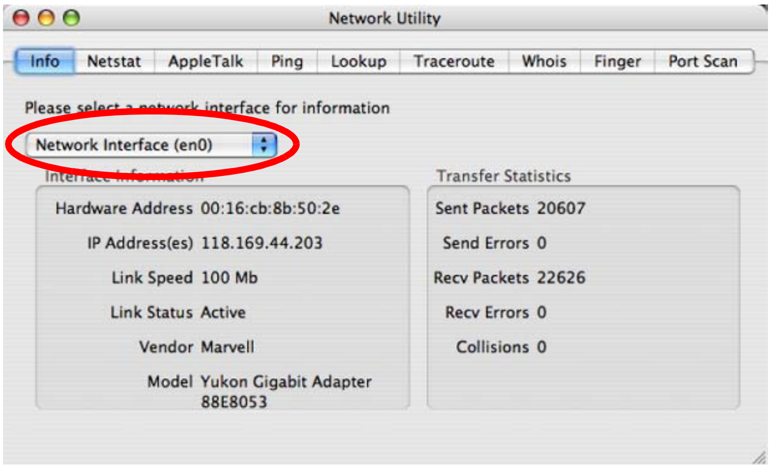


Location: Automatic
Show: Built-in Ethernet
Configure IPv4: Manually
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Router: 0.0.0.0
DNS Servers:
Search Domains:
IPv6 Address:

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 145 Mac OS X 10.4: Network Utility



Network Interface (en0)

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

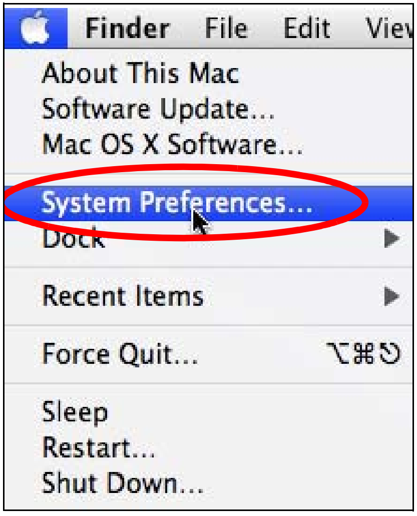
Sent Packets 20607
Send Errors 0
Recv Packets 22626
Recv Errors 0
Collisions 0

Mac OS X: 10.5

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

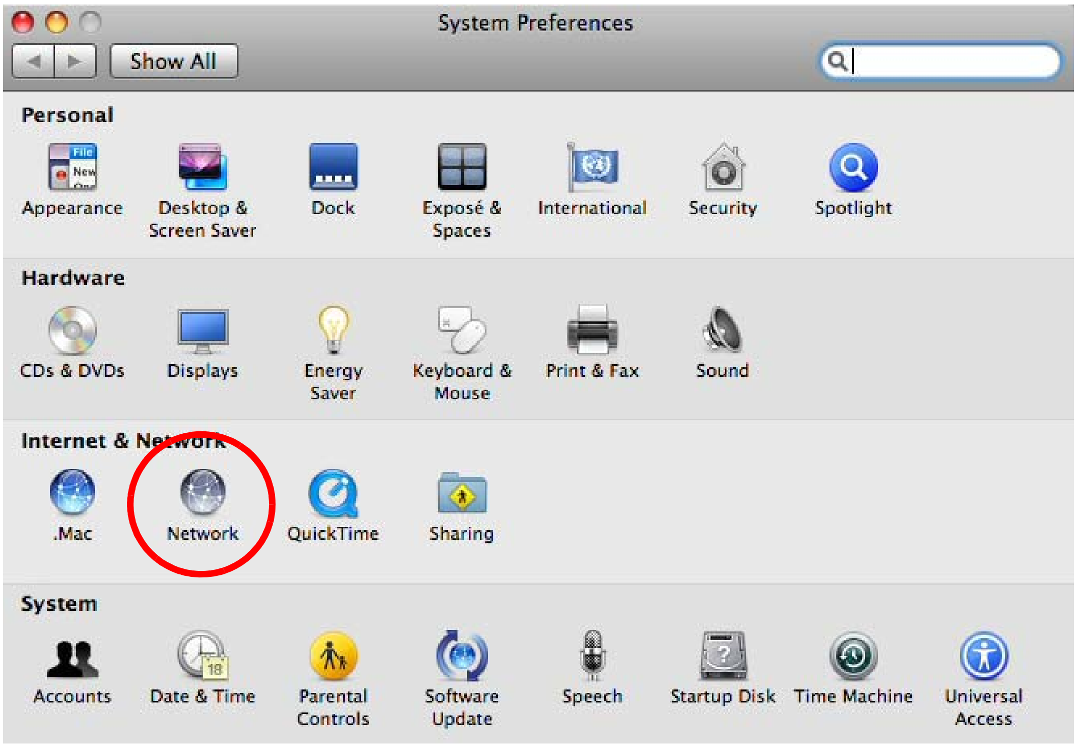
1 Click **Apple** > **System Preferences**.

Figure 146 Mac OS X 10.5: Apple Menu



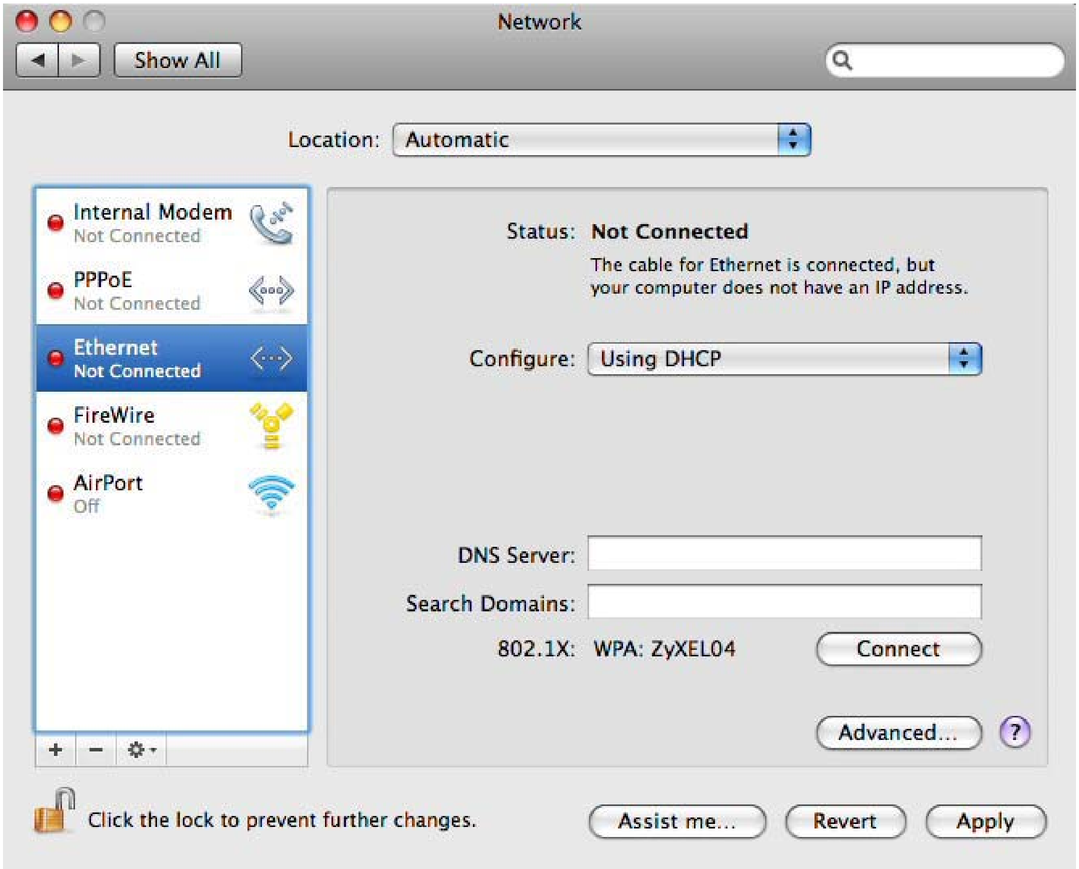
2 In **System Preferences**, click the **Network** icon.

Figure 147 Mac OS X 10.5: Systems Preferences



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

Figure 148 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

Click the lock to prevent further changes.

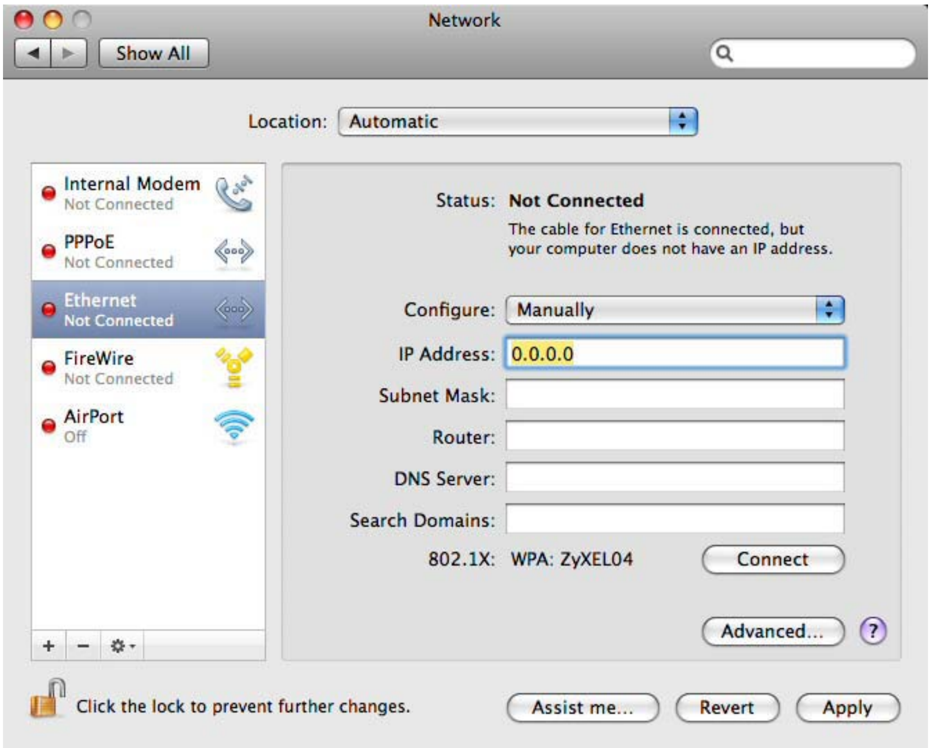
4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

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 BM2022w.

Figure 149 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: Manually

IP Address: 0.0.0.0

Subnet Mask:

Router:

DNS Server:

Search Domains:

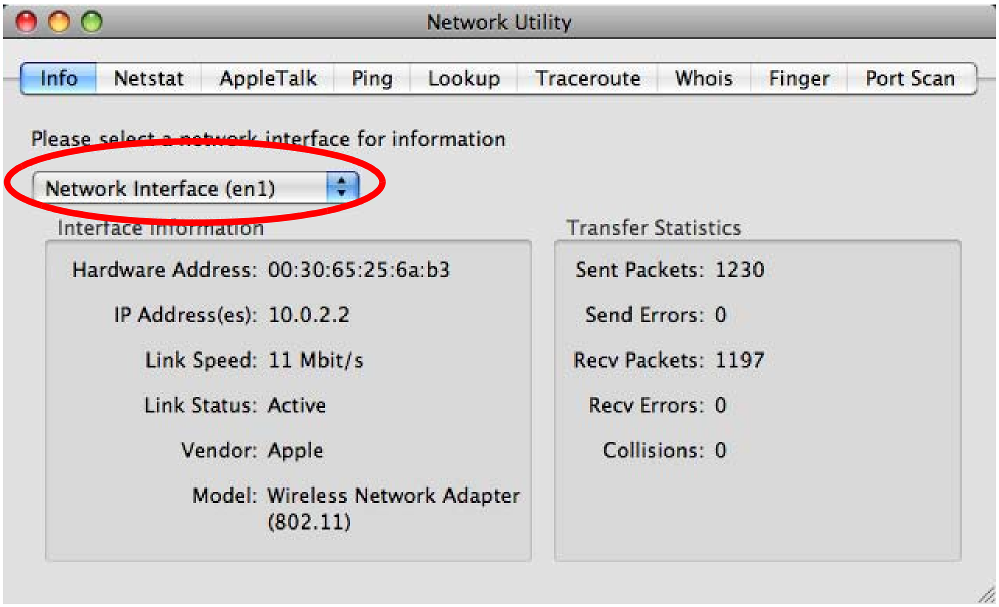
802.1X: WPA: ZyXEL04

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 150 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)

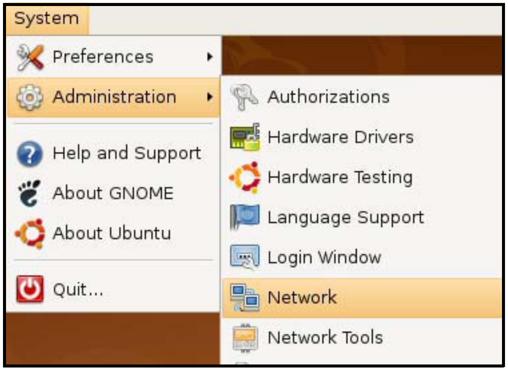
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

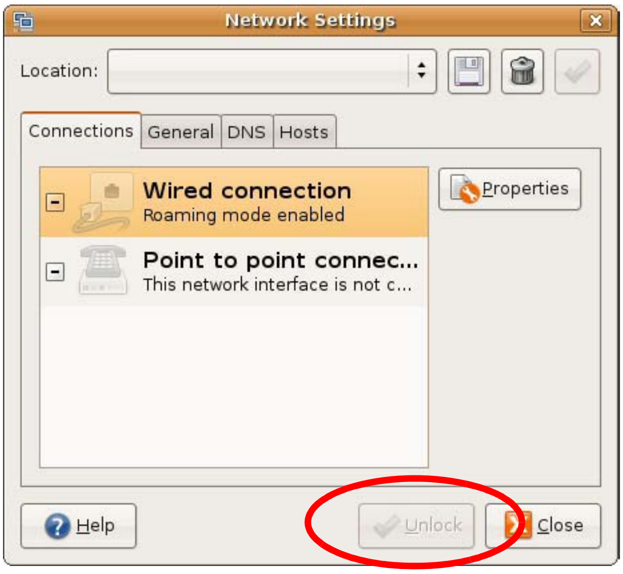
1 Click **System > Administration > Network**.

Figure 151 Ubuntu 8: System > Administration Menu



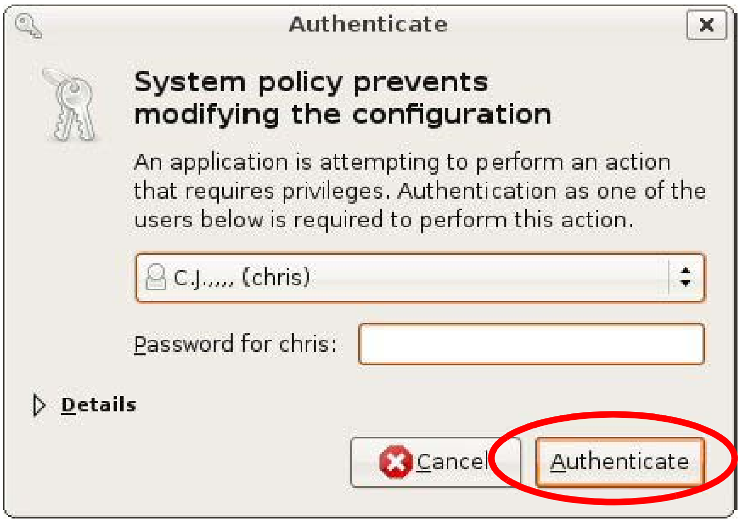
2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 152 Ubuntu 8: Network Settings > Connections



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

Figure 153 Ubuntu 8: Administrator Account Authentication



System policy prevents modifying the configuration

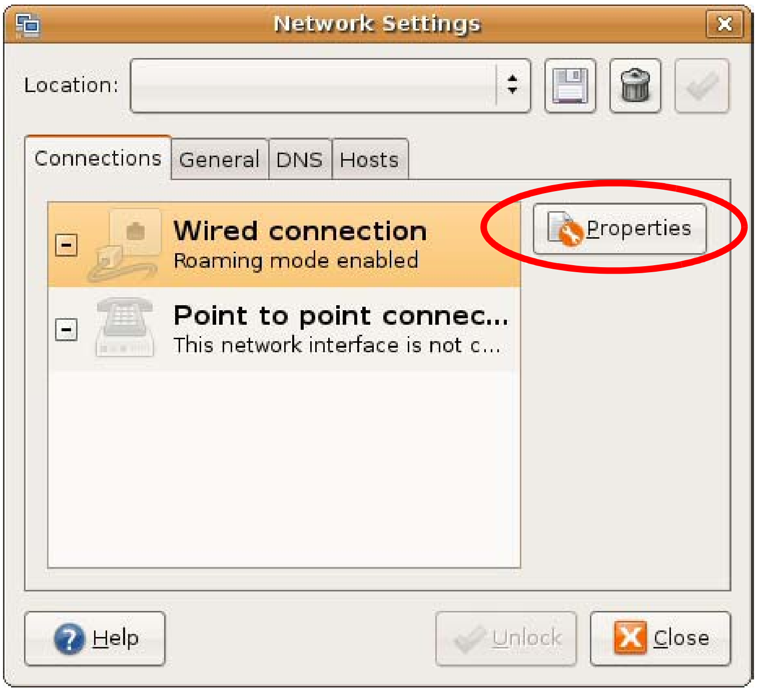
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.

C.J.,,,, (chris)

Password for chris:

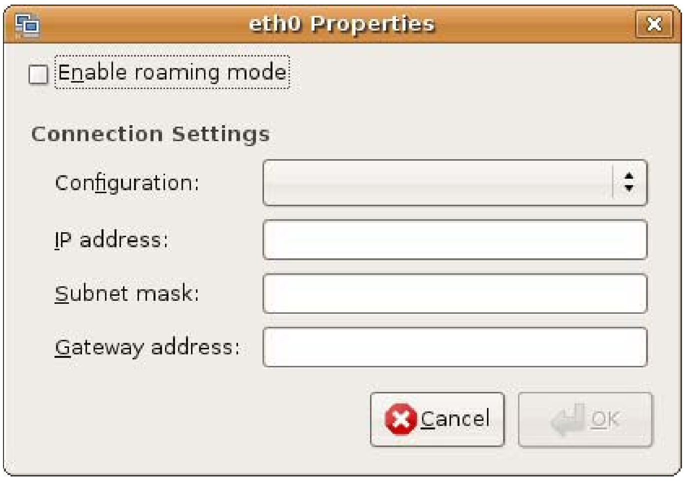
4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 154 Ubuntu 8: Network Settings > Connections



5 The **Properties** dialog box opens.

Figure 155 Ubuntu 8: Network Settings > Properties

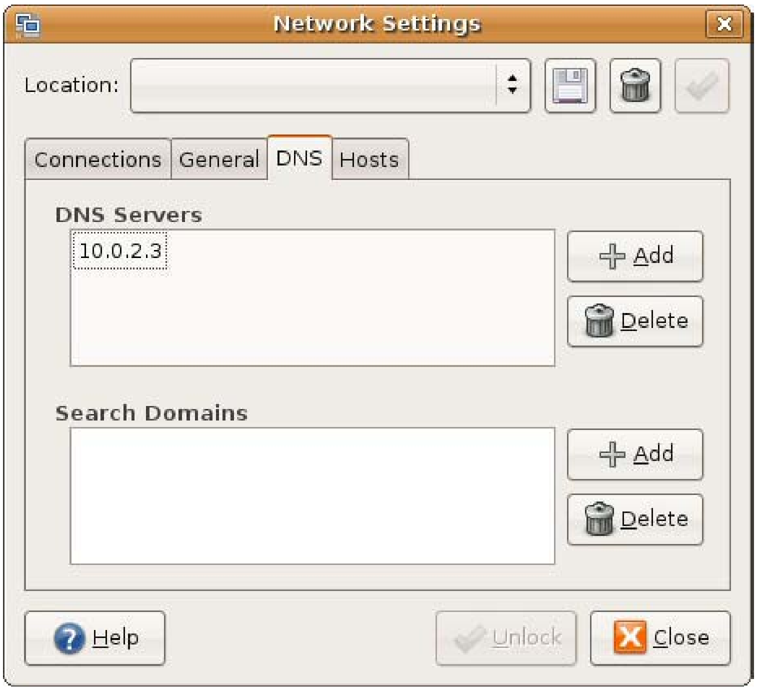


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

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 156 Ubuntu 8: Network Settings > DNS



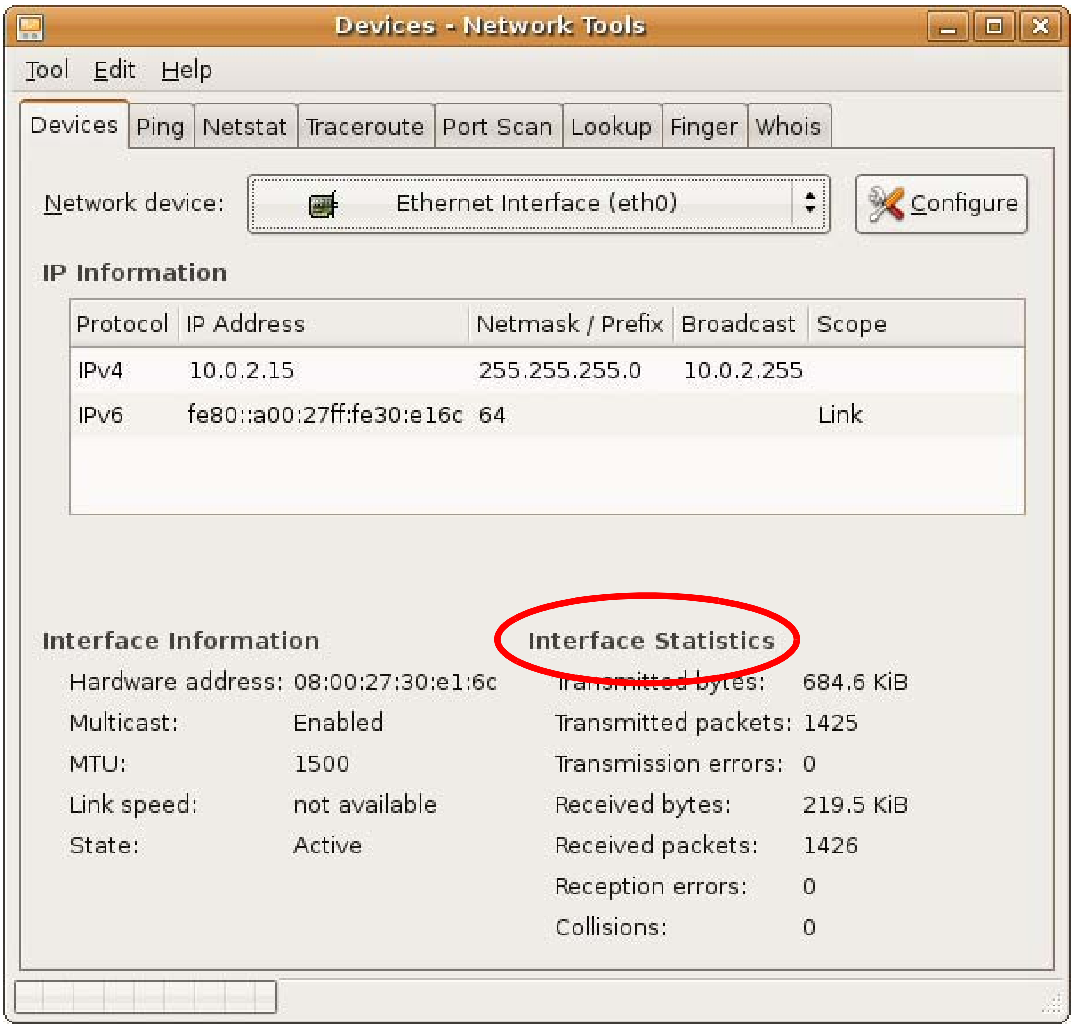
10.0.2.3

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 157 Ubuntu 8: Network Tools



Devices - Network Tools
Tool Edit Help
Devices Ping Netstat Traceroute Port Scan Lookup Finger Whois
Configure

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)

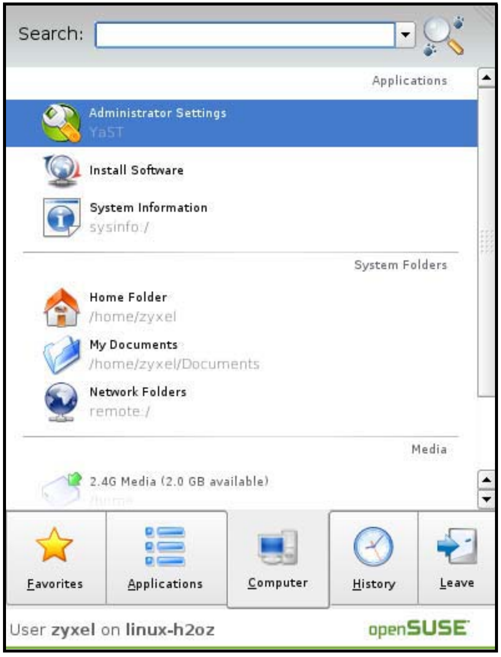
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

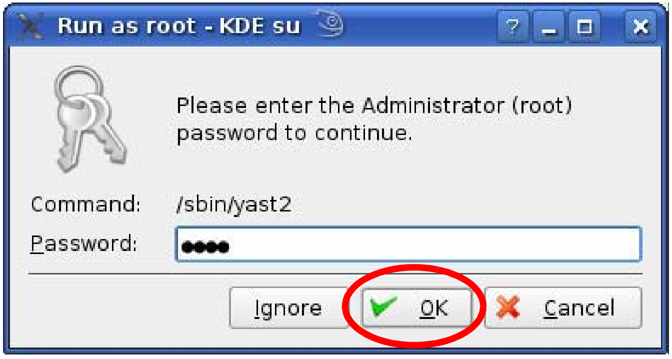
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 158 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 159 openSUSE 10.3: K Menu > Computer Menu



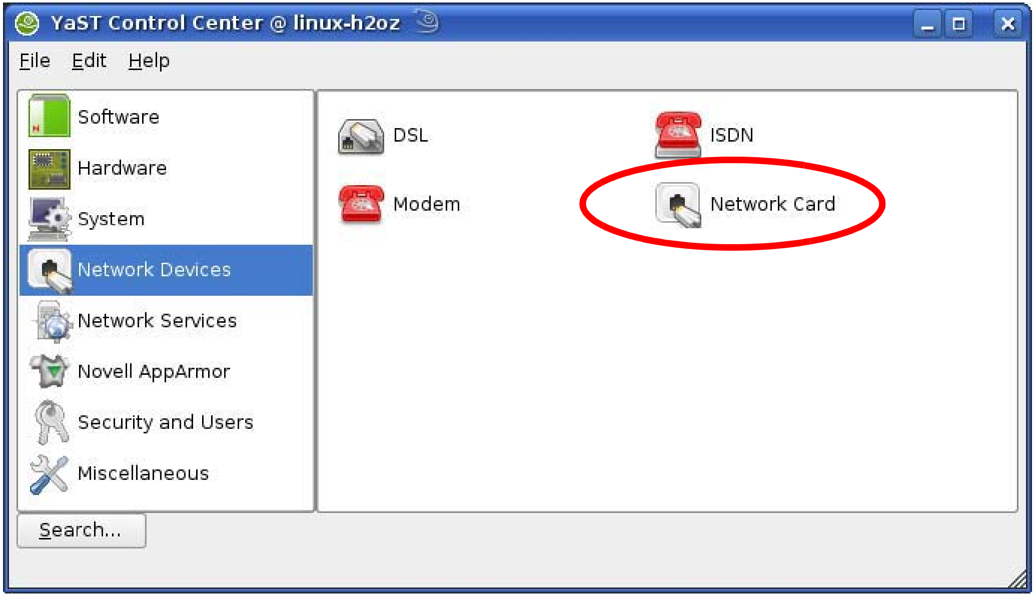
Please enter the Administrator (root) password to continue.

Command: /sbin/yast2

Password: ●●●●

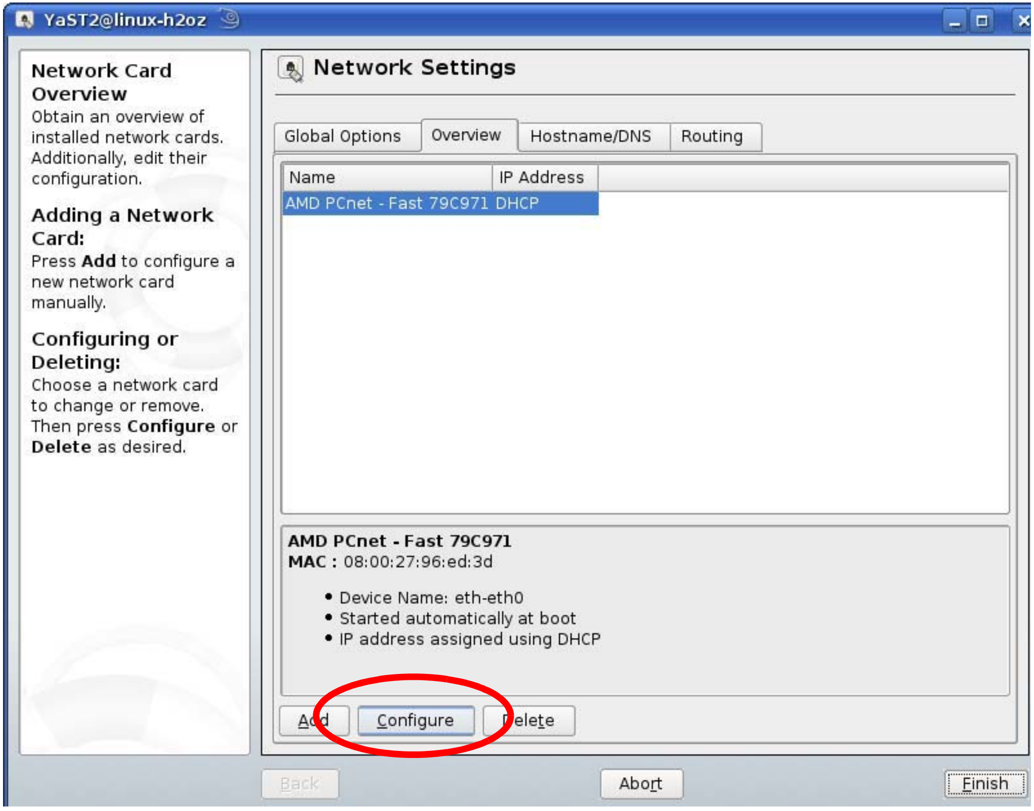
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 160 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 161 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.

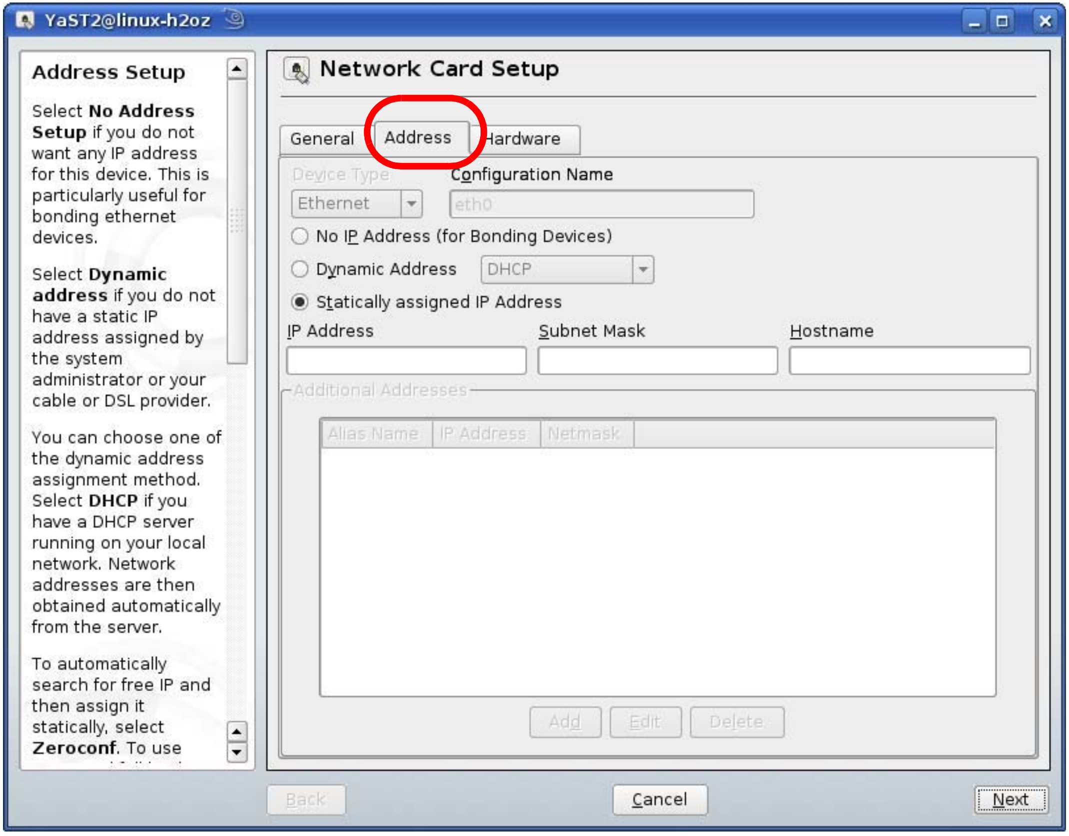
Name	IP Address
AMD PCnet - Fast 79C971	DHCP

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 162 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

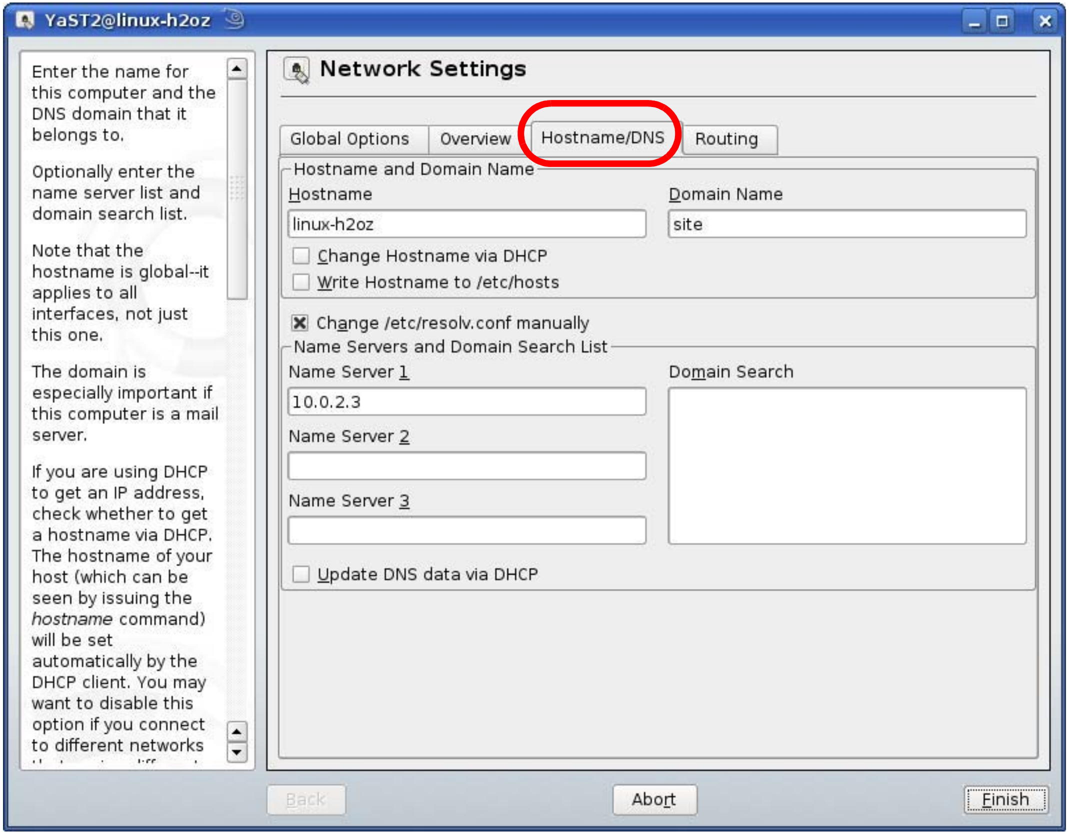
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

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 163 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:

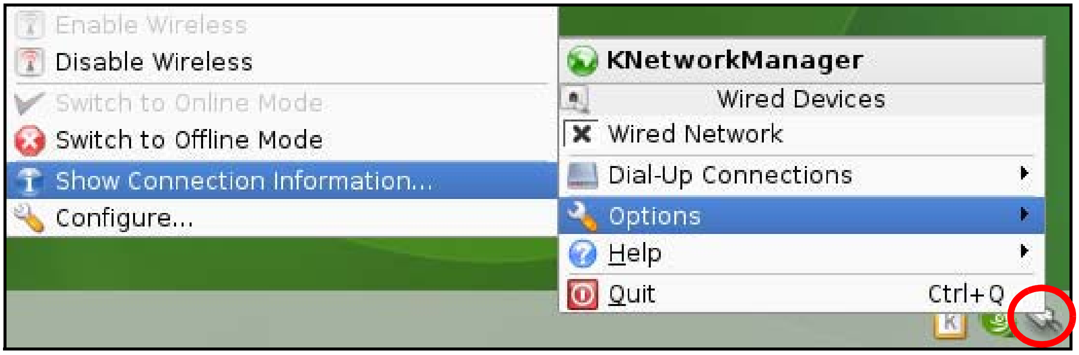
□ Update DNS data via DHCP

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

Verifying Settings

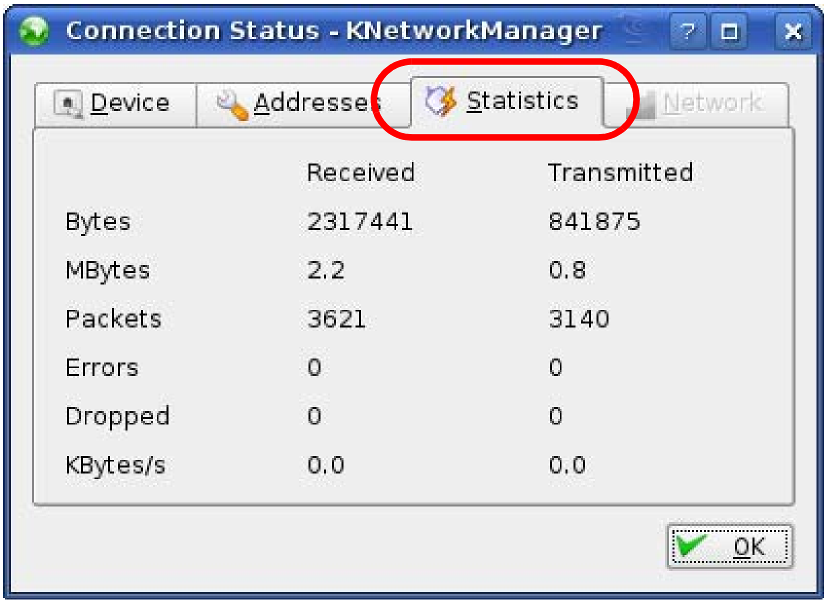
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 164 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 165 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

C

Pop-up Windows, JavaScript and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScript (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

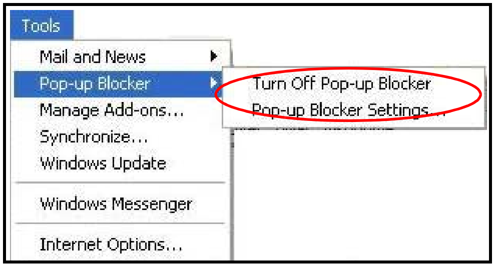
You may have to disable pop-up blocking to log into your device.

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 166 Pop-up Blocker

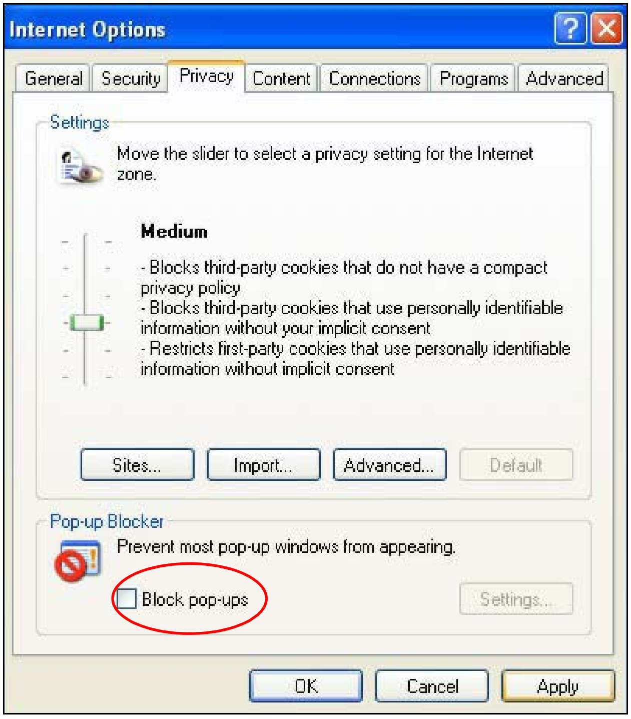


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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

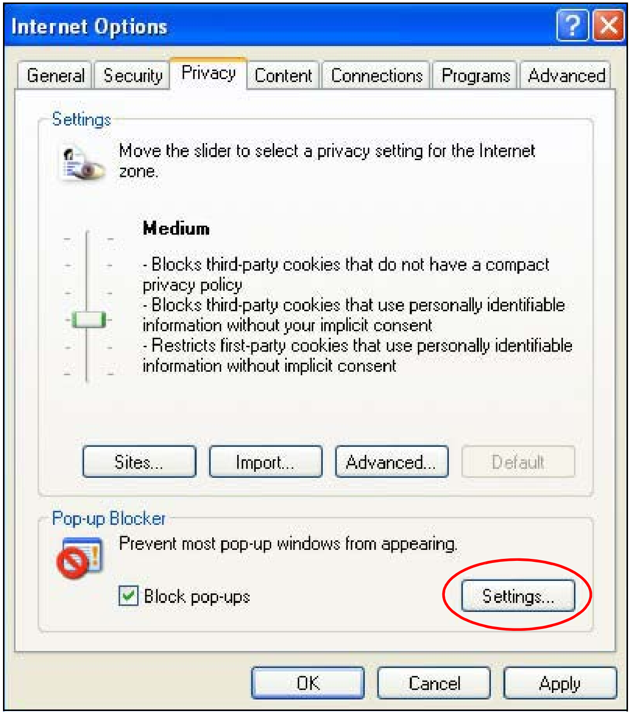
Enable Pop-up Blockers with Exceptions

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 168 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

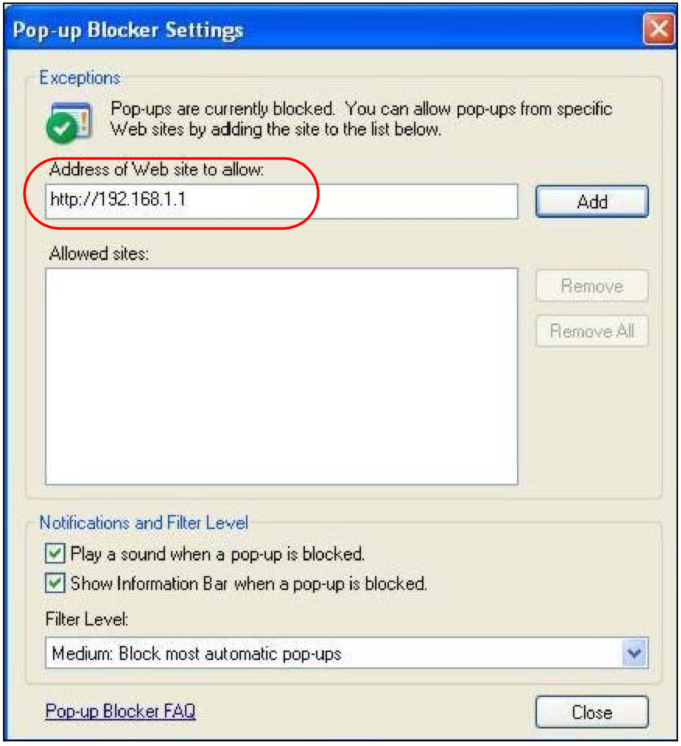
Prevent most pop-up windows from appearing.

☑ 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 169 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.

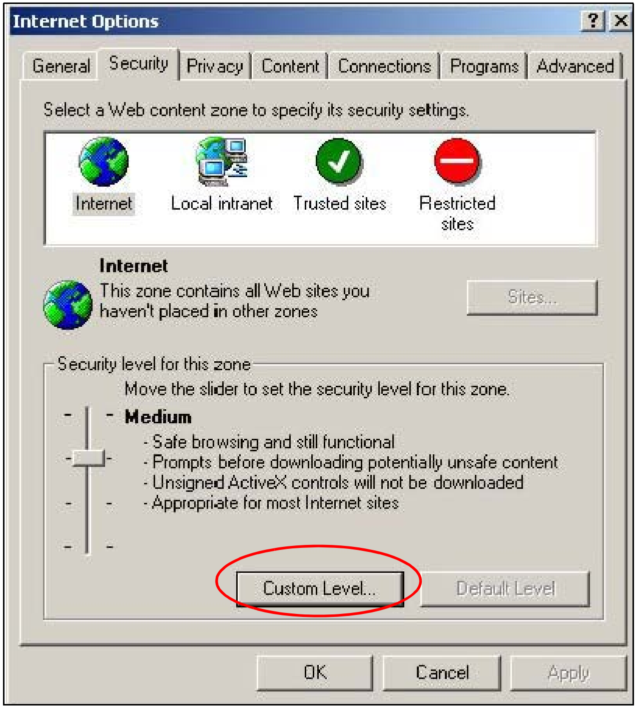
6 Click **Apply** to save this setting.

JavaScript

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

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

Figure 170 Internet Options: Security



Select a Web content zone to specify its security settings.

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

Security level for this zone

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.

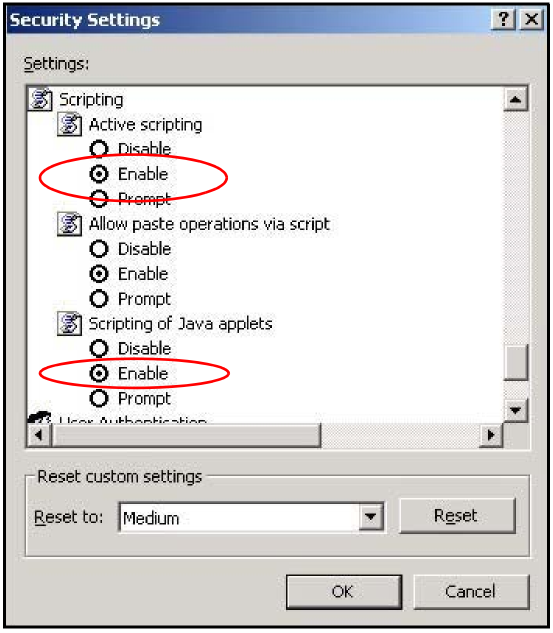
3 Scroll down to **Scripting**.

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 171 Security Settings - Java Scripting



Settings:

Scripting

Active scripting

- ○ Disable
- ● Enable
- ○ Prompt

Allow paste operations via script

- ○ Disable
- ● Enable
- ○ Prompt

Scripting of Java applets

- ○ Disable
- ● Enable
- ○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

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

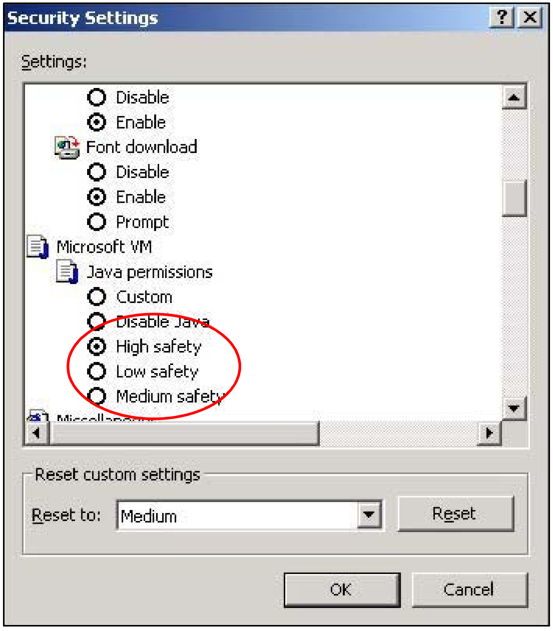
2 Click the **Custom Level...** button.

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 172 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

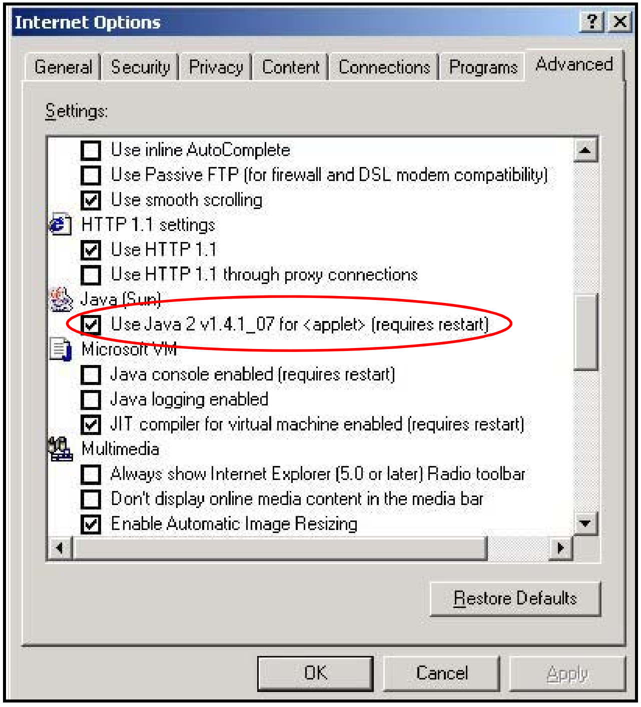
JAVA (Sun)

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 173 Java (Sun)



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings:

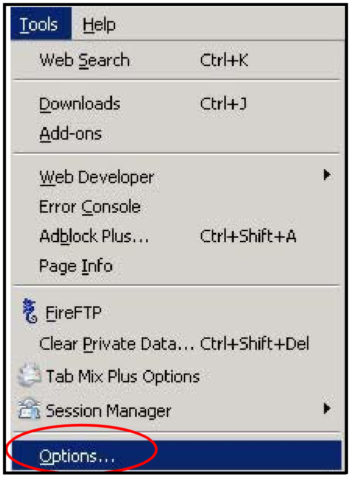
- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling
- HTTP 1.1 settings
  - ☑ Use HTTP 1.1
  - □ Use HTTP 1.1 through proxy connections
- Java (Sun)
  - ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
- Microsoft VM
  - □ Java console 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.

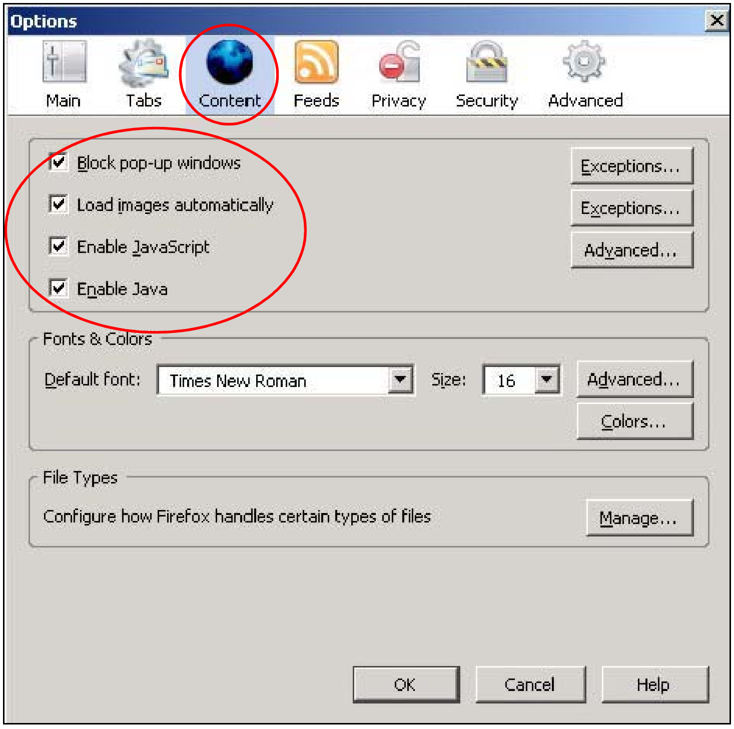
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 174 Mozilla Firefox: TOOLS > Options



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

Figure 175 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

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.

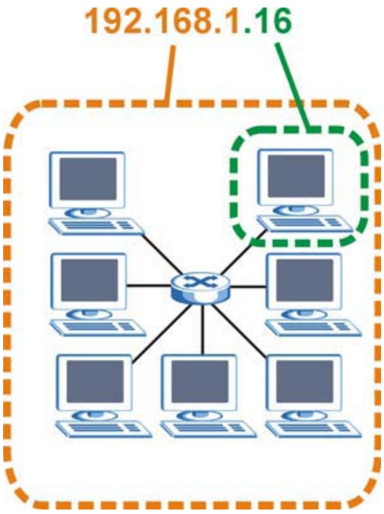
Structure

An IP address is made up of four parts, written in dotted decimal notation. 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 176 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 110 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 111 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 112 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 113 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

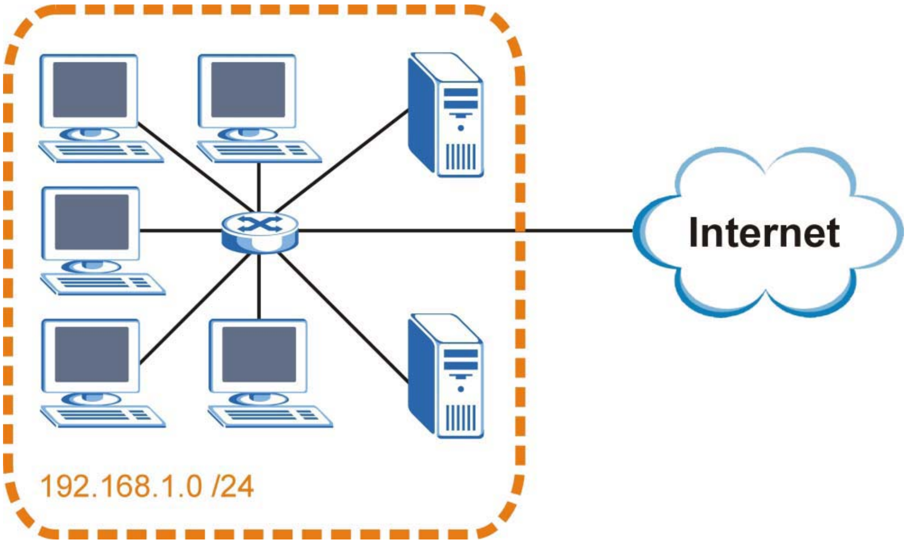
Subnetting

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 177 Subnetting Example: Before Subnetting

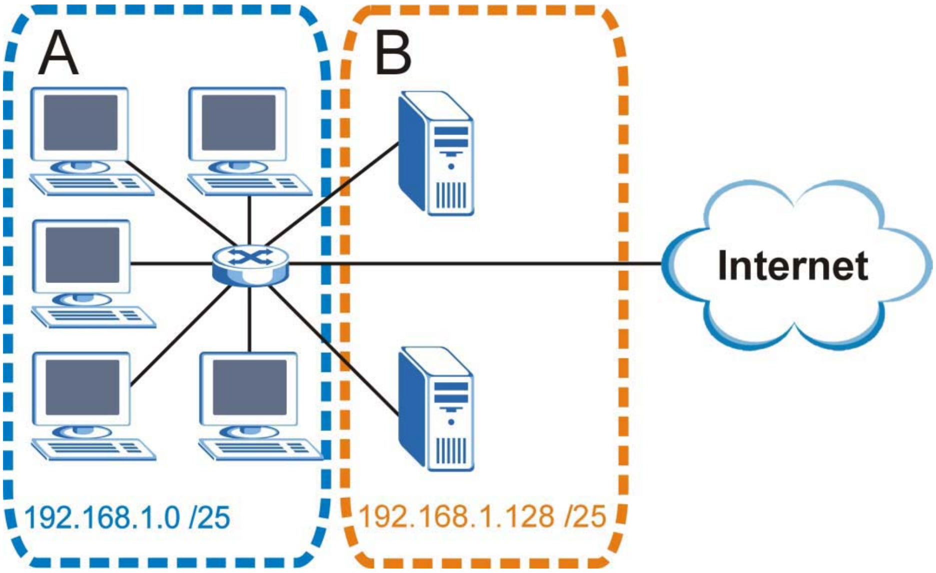


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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

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

Figure 178 Subnetting Example: After Subnetting



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

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

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

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**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 114 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

Table 114 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 115 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: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 116 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: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 117 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: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

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

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

Table 118 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 119 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 120 16-bit Network Number Subnet Planning

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

Table 120 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 BM2022w.

Once you have decided on the network number, pick an IP address for your BM2022w that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your BM2022w 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 BM2022w 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.

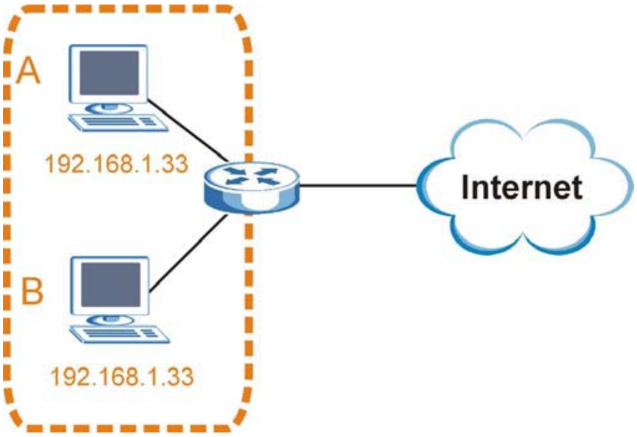
IP Address Conflicts

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.

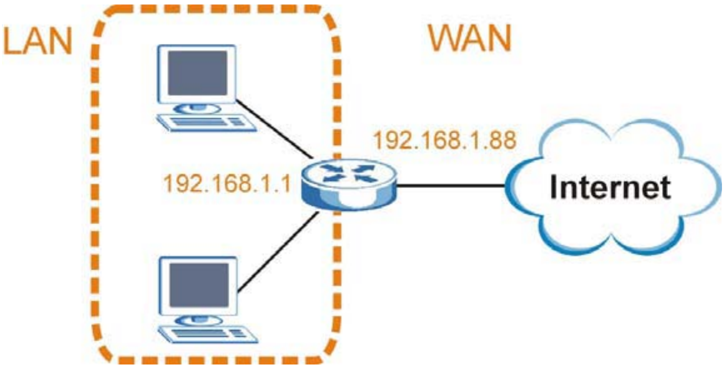
Figure 179 Conflicting Computer IP Addresses Example



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.

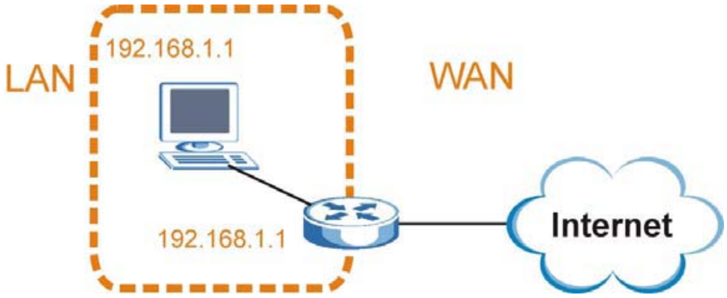
Figure 180 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 181 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 Huawei products 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 Huawei-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:

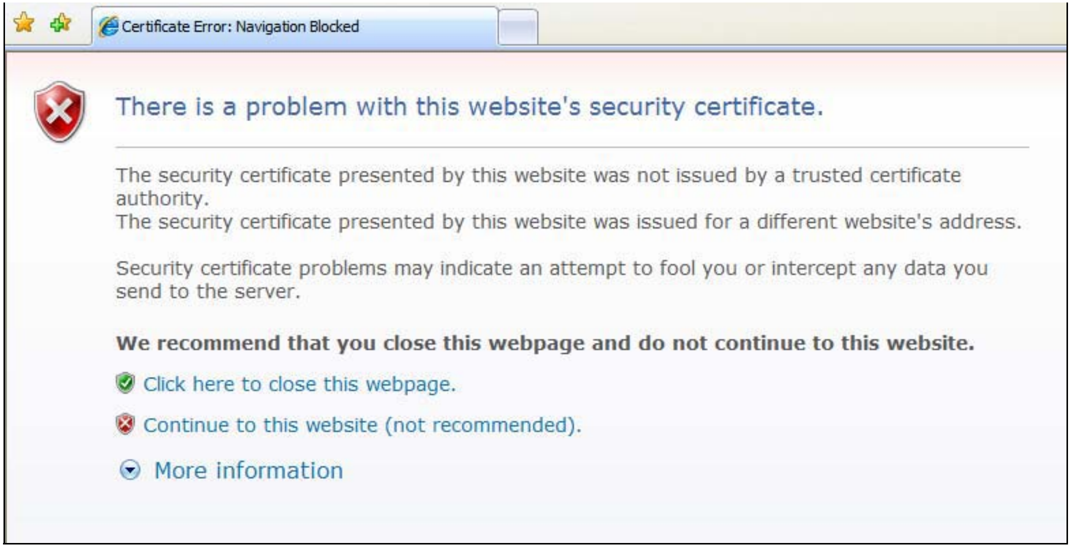
- Internet Explorer on page 264
- Firefox on page 272
- Opera on page 277
- Konqueror on page 284

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 182 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.

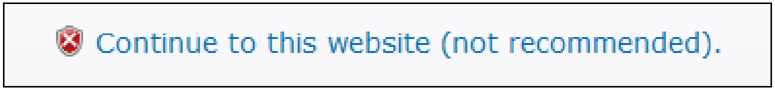
Click here to close this webpage.

Continue to this website (not recommended).

More information

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

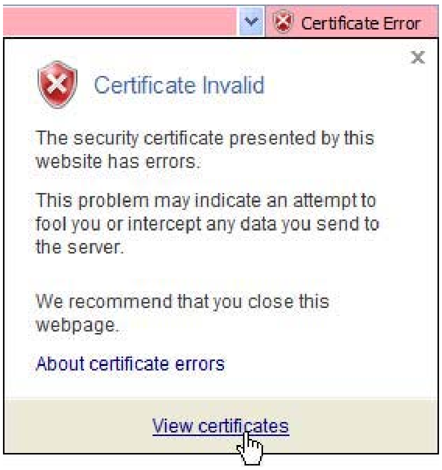
Figure 183 Internet Explorer 7: Certification Error



Continue to this website (not recommended).

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

Figure 184 Internet Explorer 7: Certificate Error



Certificate Invalid

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.

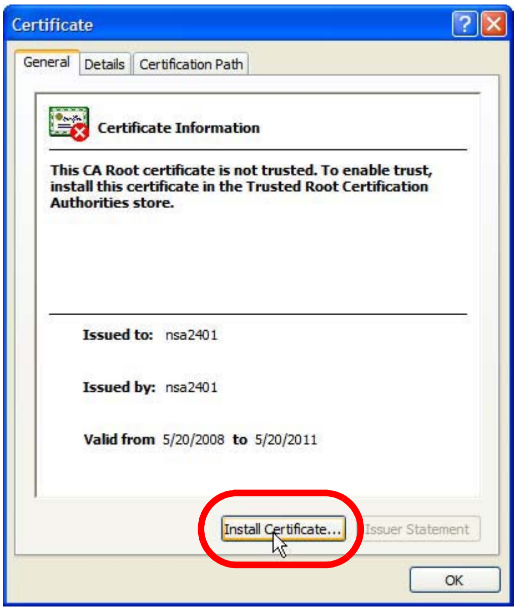
We recommend that you close this webpage.

About certificate errors

View certificates

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

Figure 185 Internet Explorer 7: Certificate



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

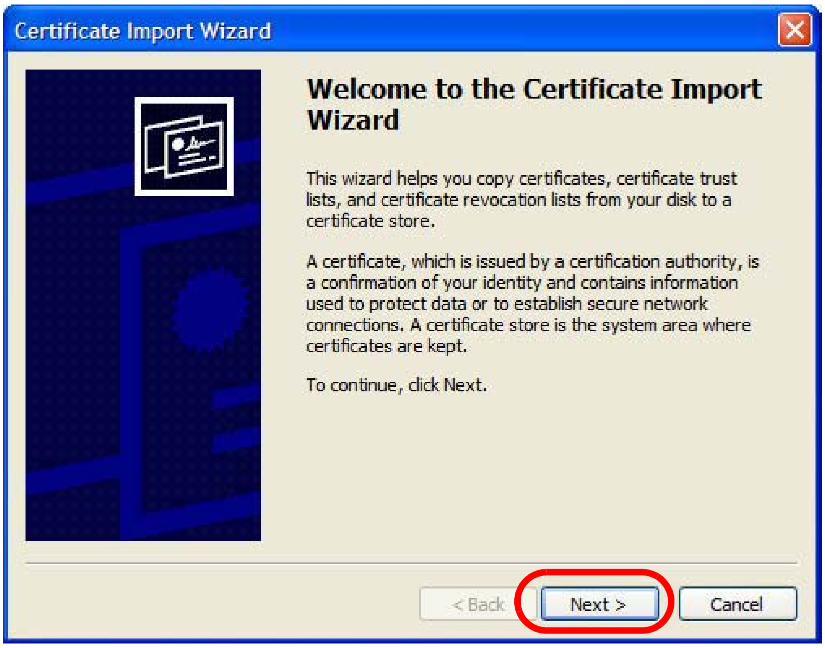
Issued to: nsa2401

Issued by: nsa2401

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

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

Figure 186 Internet Explorer 7: Certificate Import Wizard



Welcome to the Certificate Import Wizard

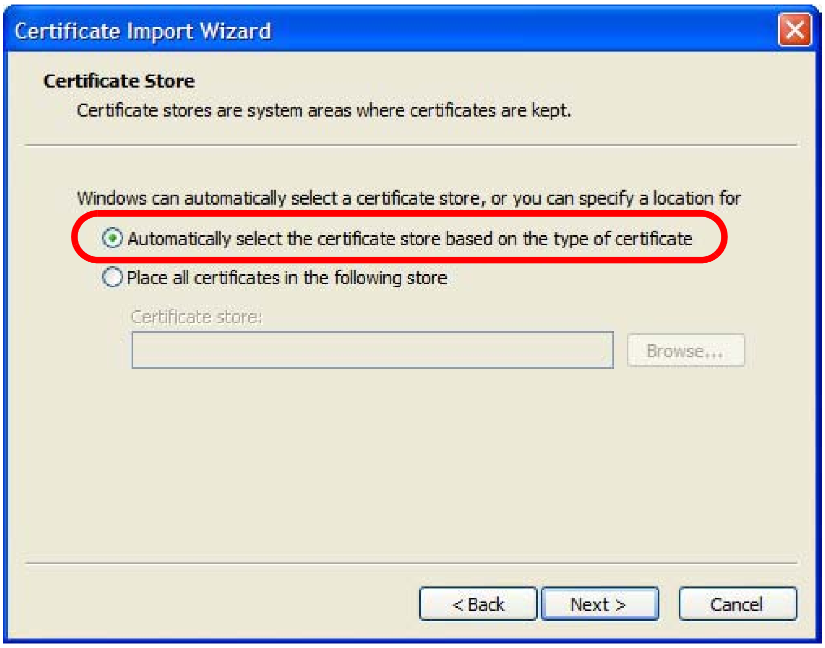
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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 187 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

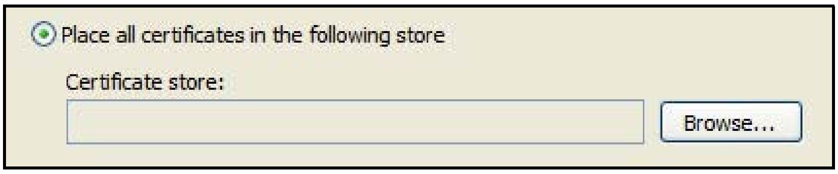
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

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

Figure 188 Internet Explorer 7: Certificate Import Wizard

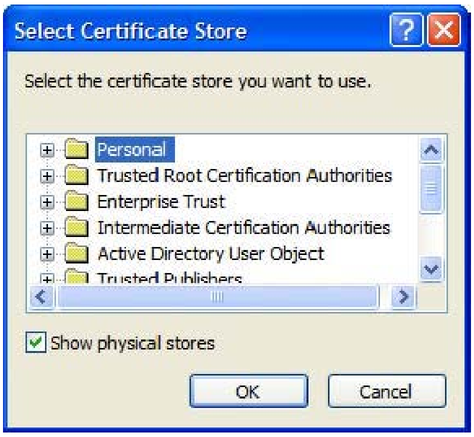


● Place all certificates in the following store

Certificate store:

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

Figure 189 Internet Explorer 7: Select Certificate Store



Select Certificate Store

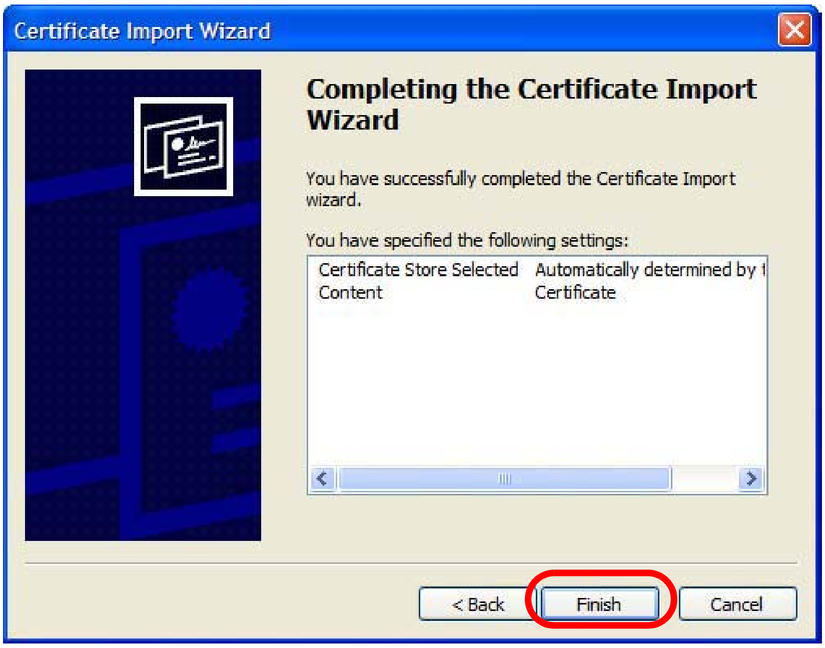
Select the certificate store you want to use.

- 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 190 Internet Explorer 7: Certificate Import Wizard



Certificate Import Wizard

Completing the Certificate Import Wizard

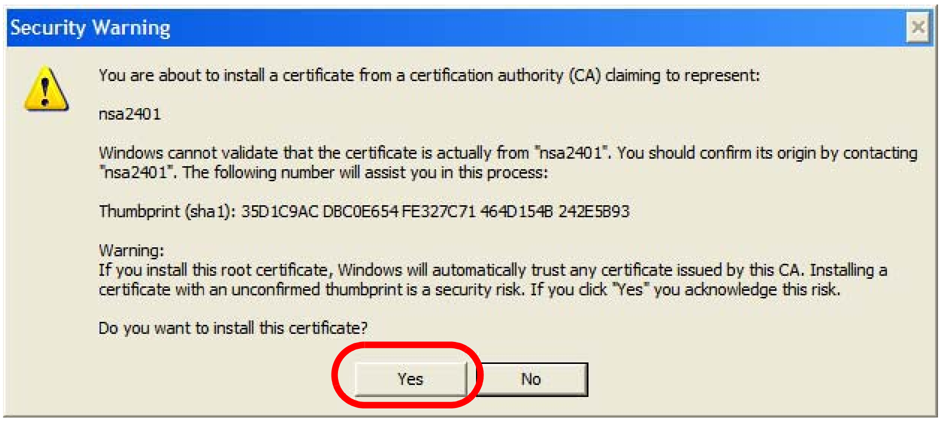
You have successfully completed the Certificate Import wizard.

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 191 Internet Explorer 7: Security Warning



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:

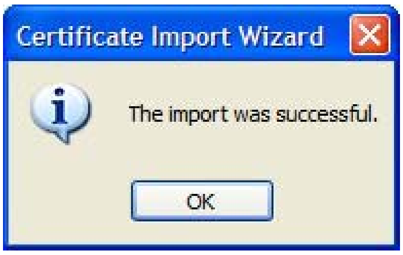
Thumbprint (sha1): 35D1C9AC DBC0E654 FE327C71 464D154B 242E5B93

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 192 Internet Explorer 7: Certificate Import Wizard

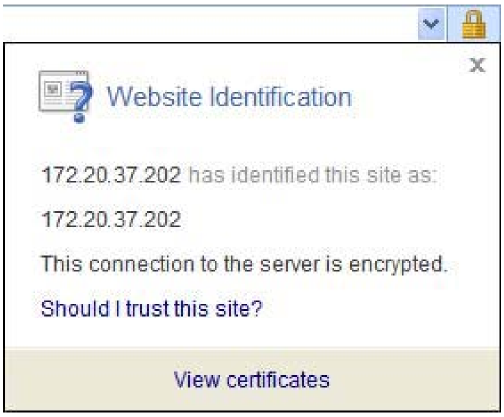


Certificate Import Wizard

The import was successful.

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

Figure 193 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.

Should I trust this site?

Installing a Stand-Alone Certificate File in Internet Explorer

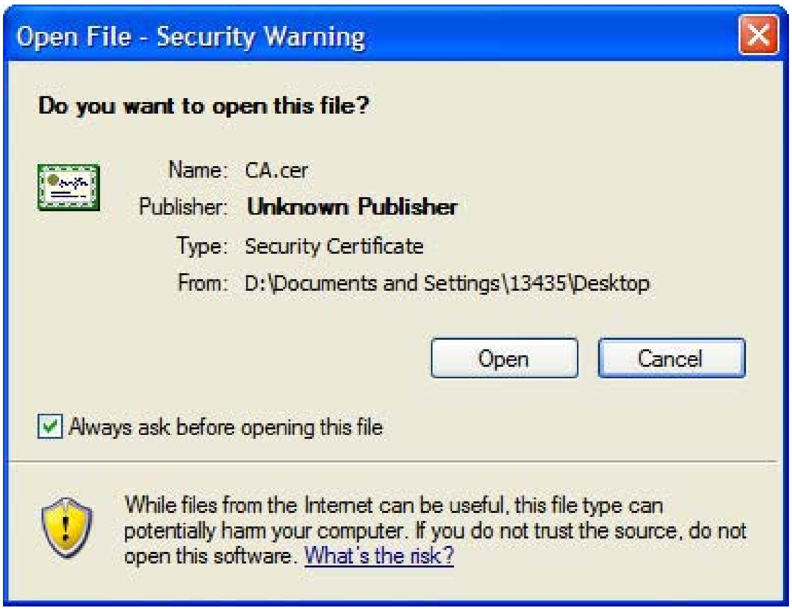
Rather than browsing to a Huawei web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 194 Internet Explorer 7: Public Key Certificate File

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

Figure 195 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?

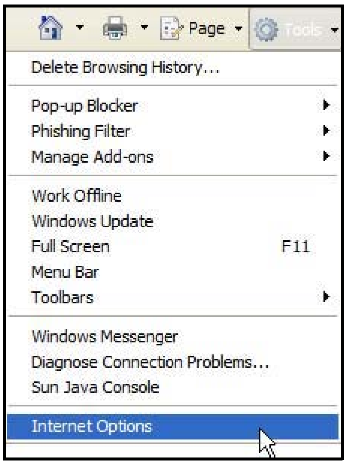
3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 264 to complete the installation process.

Removing a Certificate in Internet Explorer

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

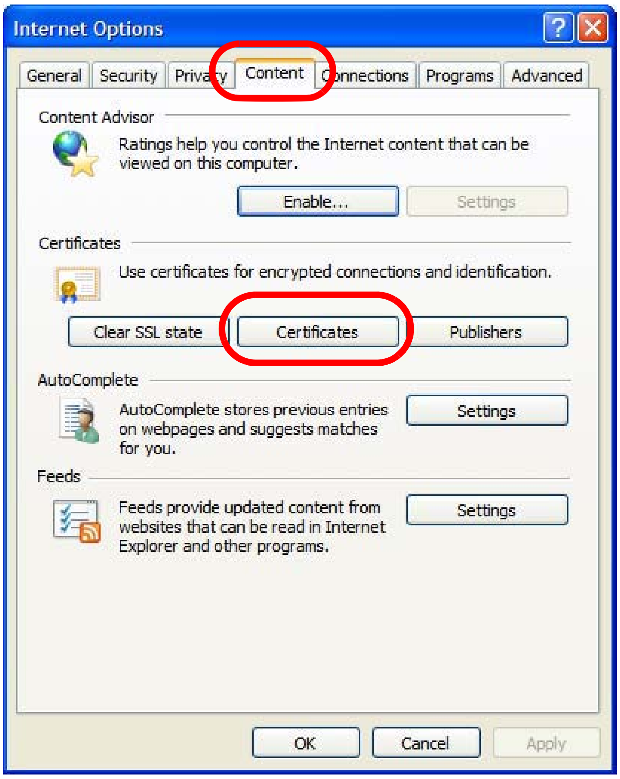
1 Open **Internet Explorer** and click **TOOLS > Internet Options**.

Figure 196 Internet Explorer 7: Tools Menu



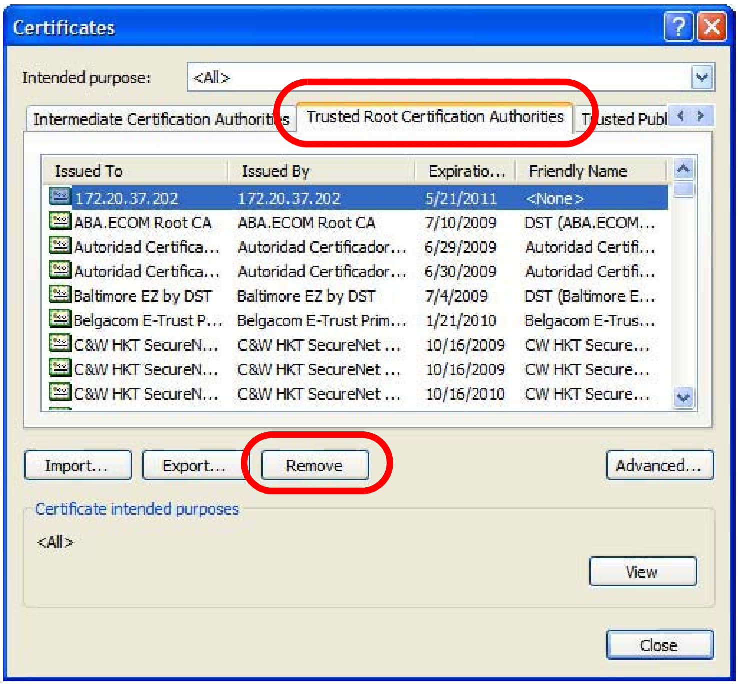
2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

Figure 197 Internet Explorer 7: Internet Options


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
Enable...
Settings
Certificates
Use certificates for encrypted connections and identification.
Clear SSL state
Certificates
Publishers
AutoComplete
AutoComplete stores previous entries on webpages and suggests matches for you.
Settings
Feeds
Feeds provide updated content from websites that can be read in Internet Explorer and other programs.
Settings
OK
Cancel
Apply

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 198 Internet Explorer 7: Certificates

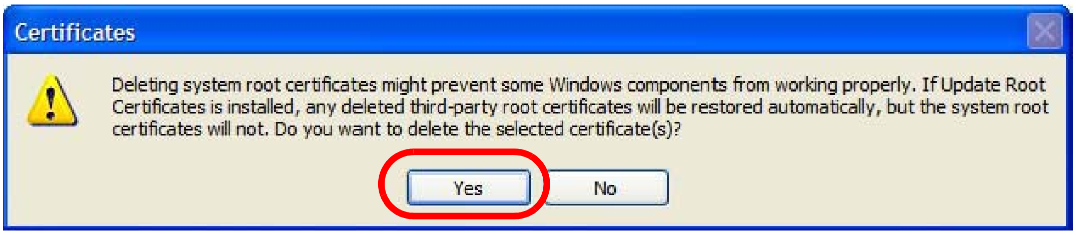


Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
<All>
View
Close

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...

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

Figure 199 Internet Explorer 7: Certificates

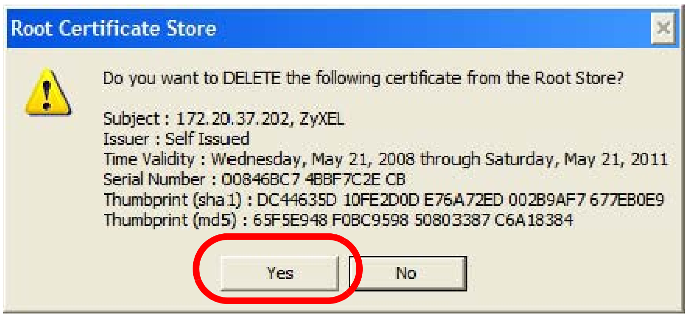


Certificates

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 200 Internet Explorer 7: Root Certificate Store



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.

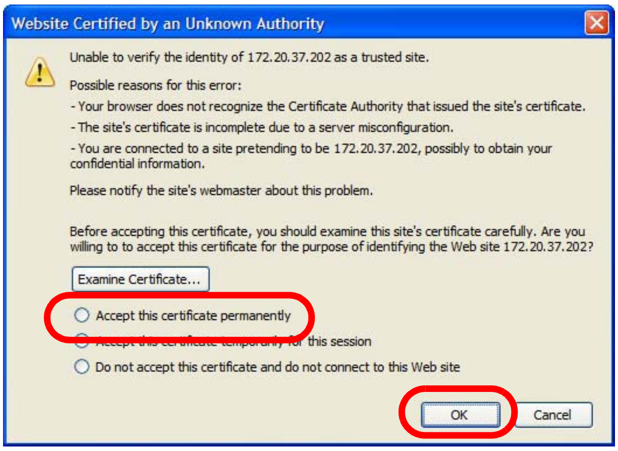
Firefox

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 201 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.

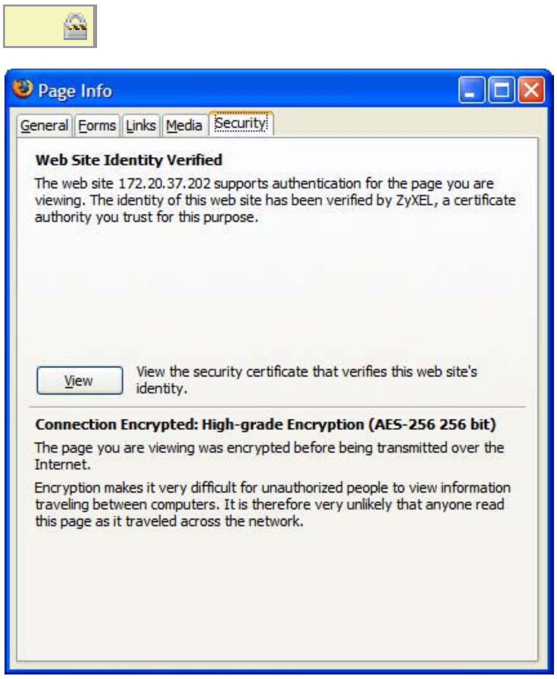
Please notify the site's webmaster about this problem.

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?

○ Accept this certificate permanently
○ Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this Web site

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 202 Firefox 2: Page Info



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.

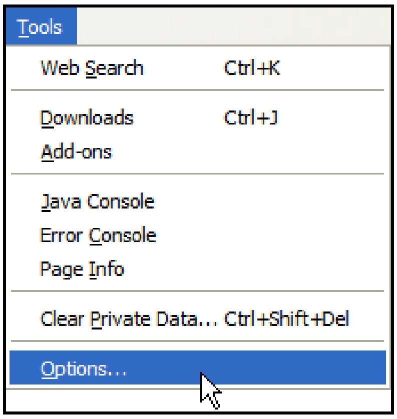
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a Huawei 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.

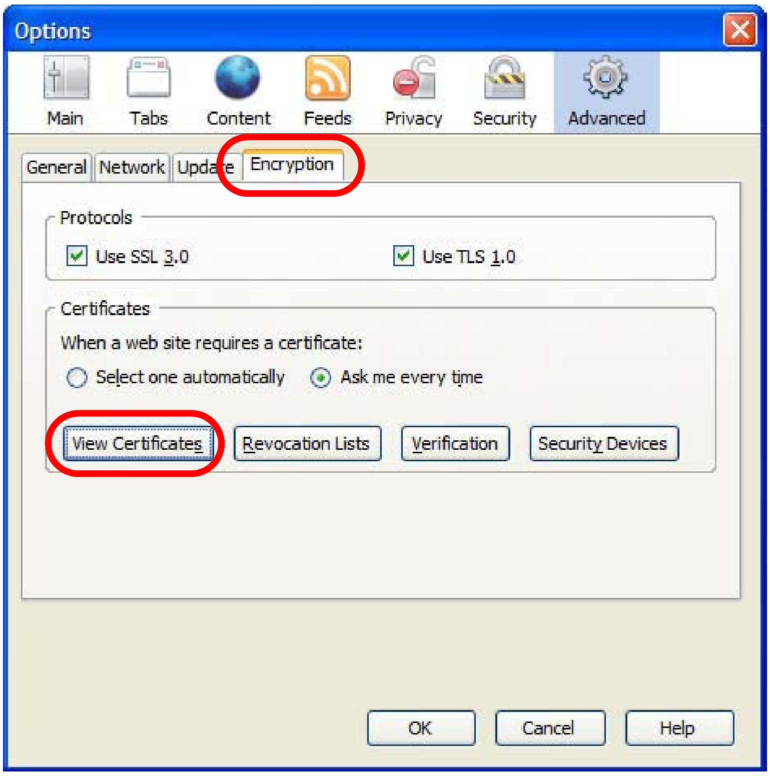
1 Open **Firefox** and click **TOOLS > Options**.

Figure 203 Firefox 2: Tools Menu



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

Figure 204 Firefox 2: Options



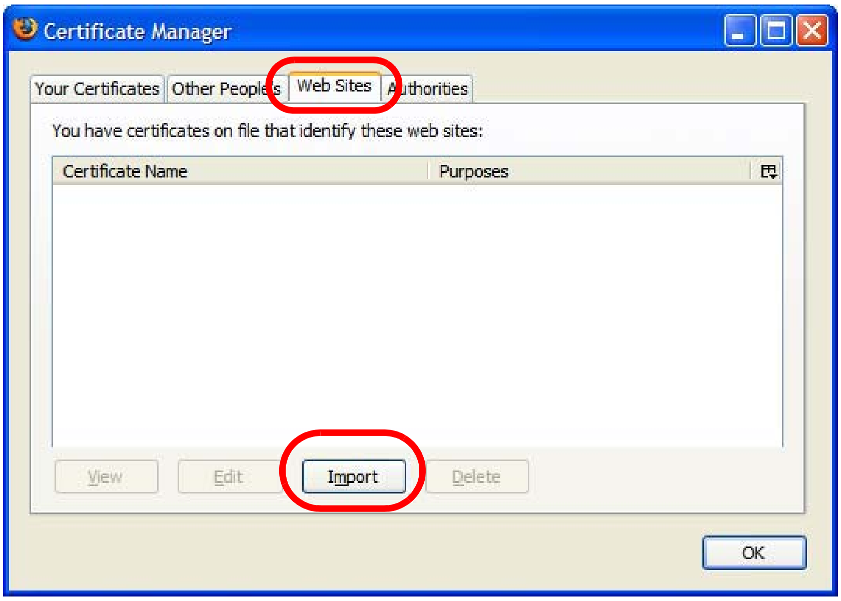
☑ Use SSL 3.0 ☑ Use TLS 1.0

When a web site requires a certificate:

○ Select one automatically ● Ask me every time

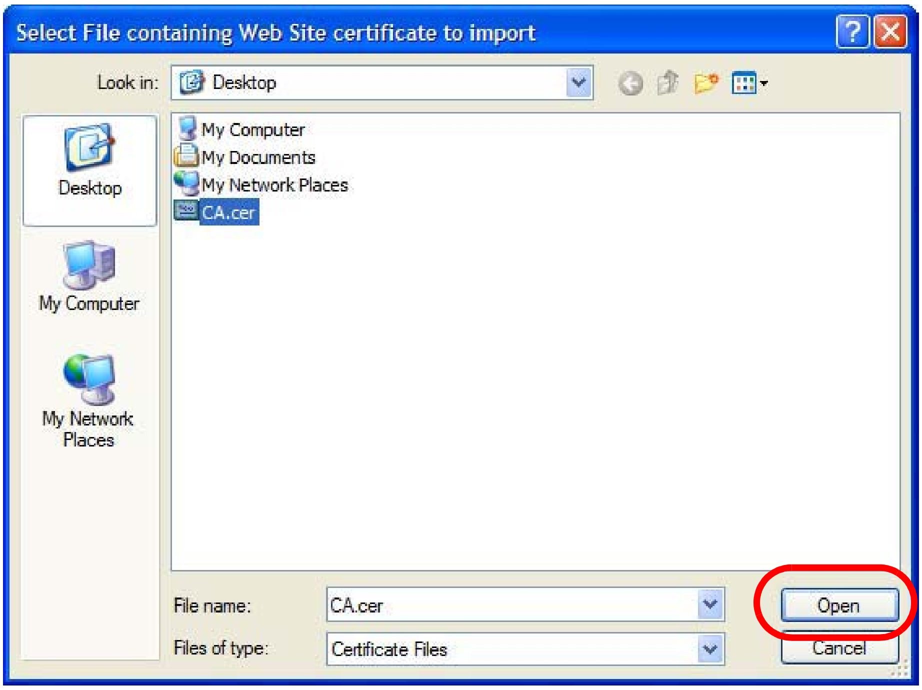
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

Figure 205 Firefox 2: Certificate Manager



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

Figure 206 Firefox 2: Select File



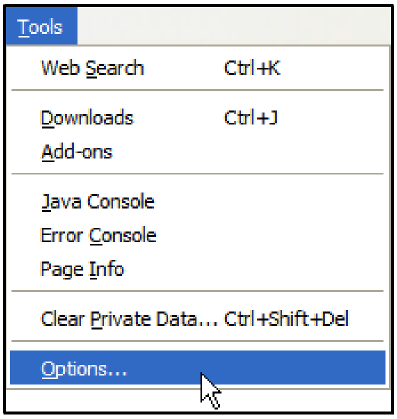
5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

Removing a Certificate in Firefox

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

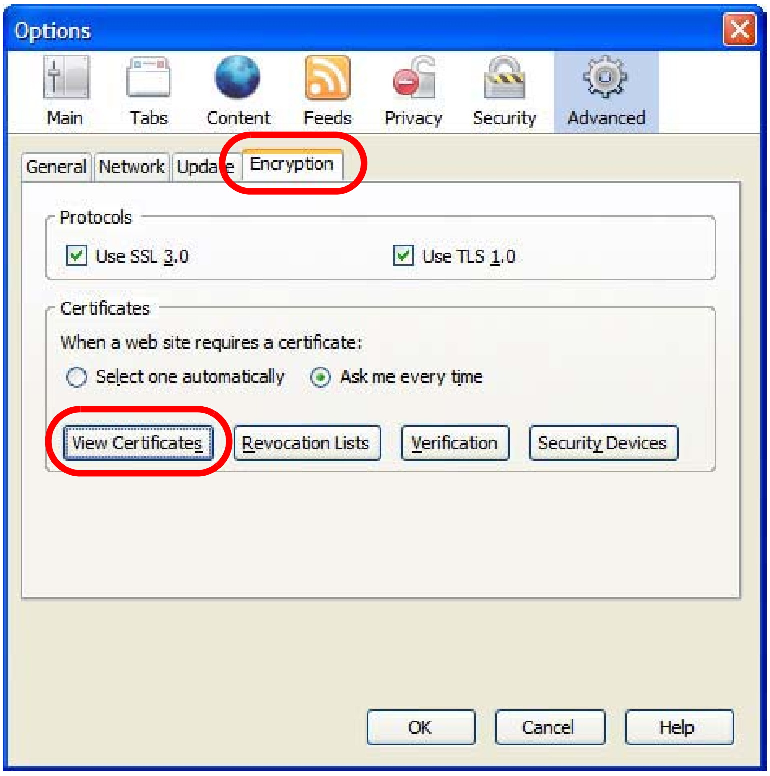
1 Open **Firefox** and click **TOOLS > Options**.

Figure 207 Firefox 2: Tools Menu



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

Figure 208 Firefox 2: Options



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

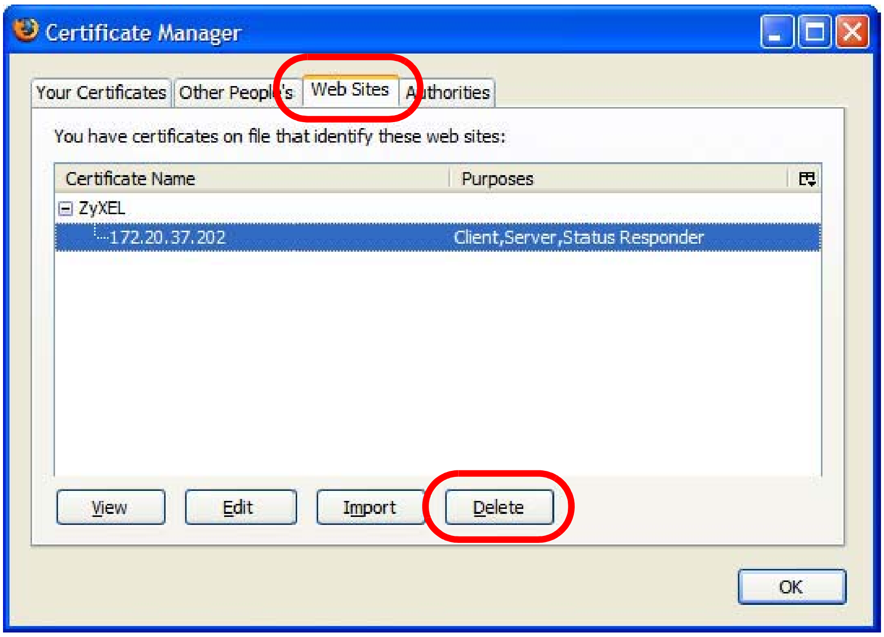
Certificates

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 209 Firefox 2: Certificate Manager

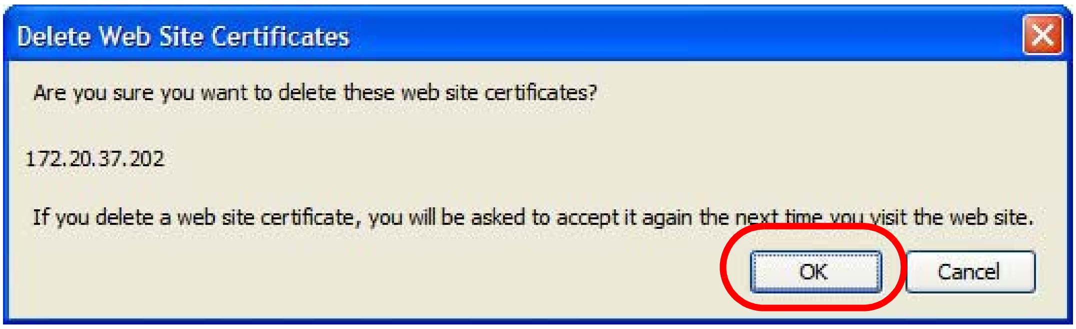


You have certificates on file that identify these web sites:

Certificate Name	Purposes
⊟ ZyXEL	
172.20.37.202	Client,Server,Status Responder

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

Figure 210 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.

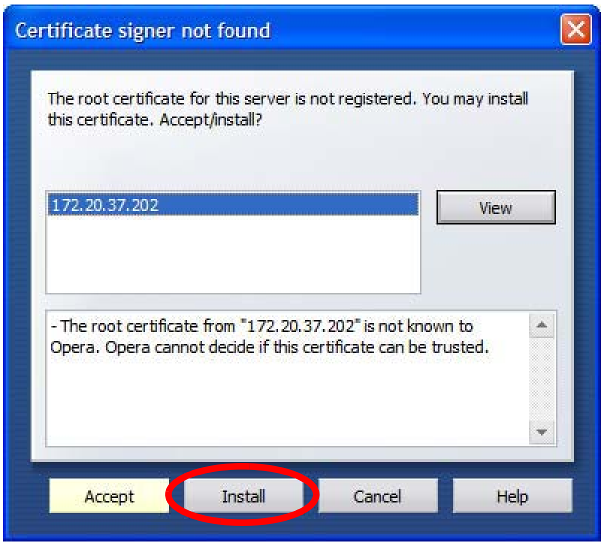
Opera

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 211 Opera 9: Certificate signer not found



Certificate signer not found

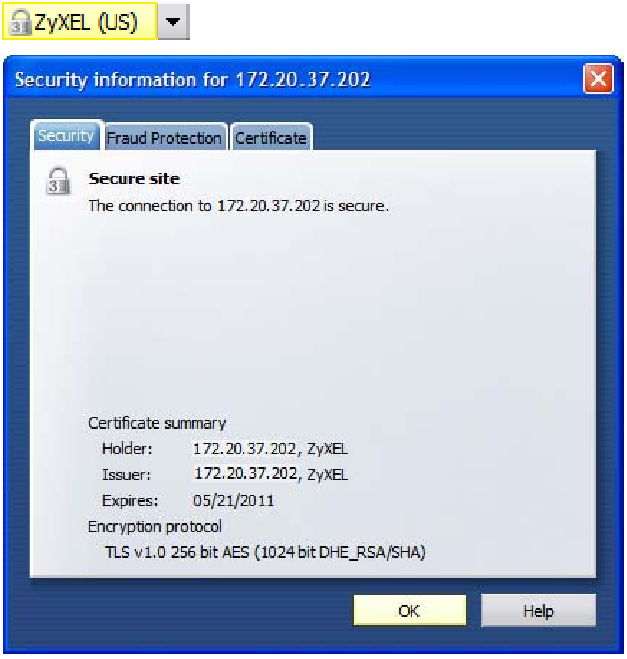
The root certificate for this server is not registered. You may install this certificate. Accept/install?

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 212 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

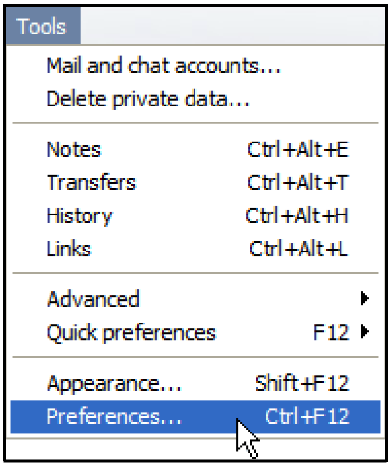
TLS v1.0 256 bit AES (1024 bit DHE_RSA/SHA)

Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a Huawei 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.

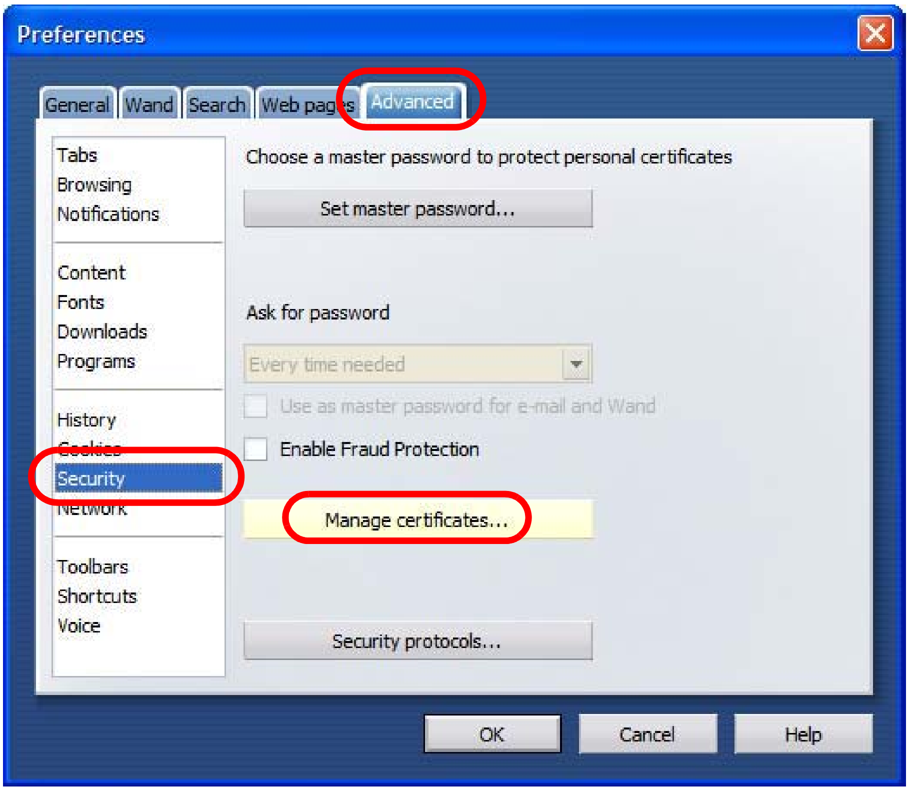
1 Open **Opera** and click **TOOLS > Preferences**.

Figure 213 Opera 9: Tools Menu



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

Figure 214 Opera 9: Preferences



Choose a master password to protect personal certificates

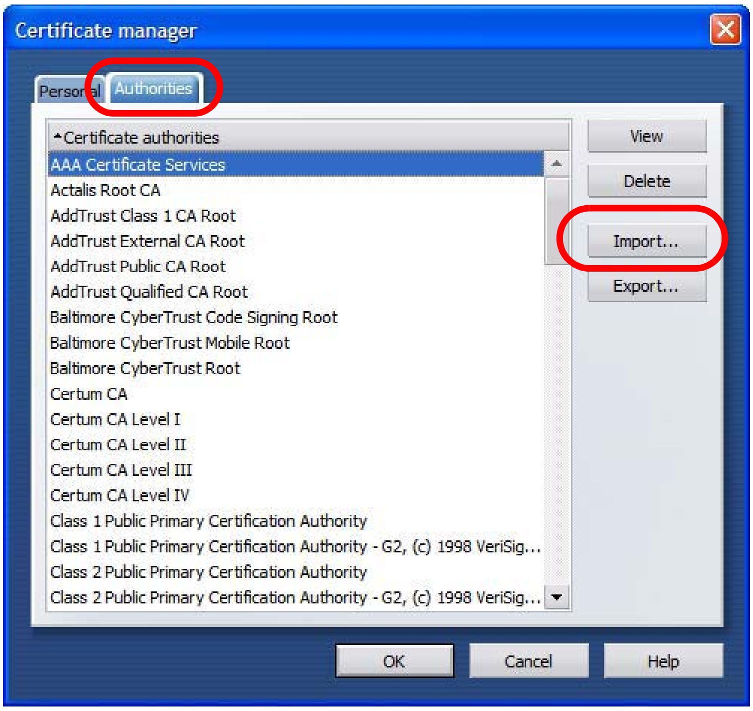
Ask for password: Every time needed

☐ Use as master password for e-mail and Wand

☐ Enable Fraud Protection

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

Figure 215 Opera 9: Certificate manager

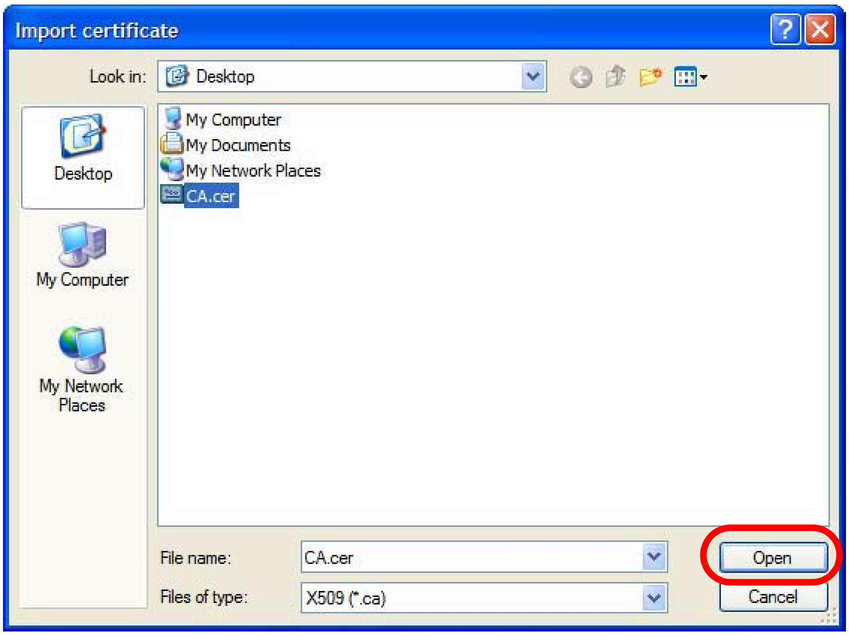


Certificate authorities

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 216 Opera 9: Import certificate



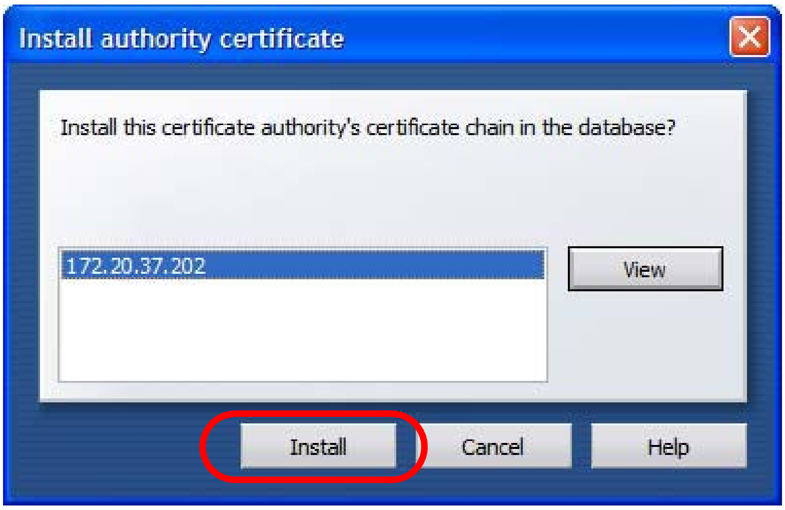
Look in: Desktop

File name: CA.cer

Files of type: X509 (*.ca)

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

Figure 217 Opera 9: Install authority certificate



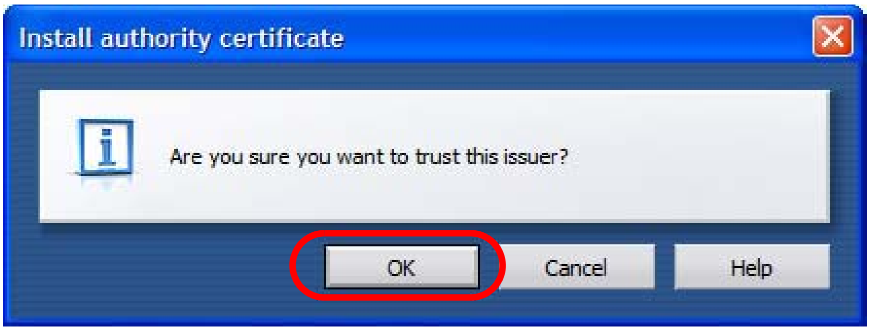
Install authority certificate

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

172.20.37.202

6 Next, click **OK**.

Figure 218 Opera 9: Install authority certificate



Install authority certificate

Are you sure you want to trust this issuer?

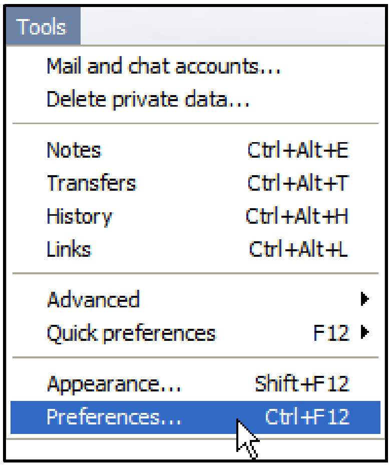
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page’s security details.

Removing a Certificate in Opera

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

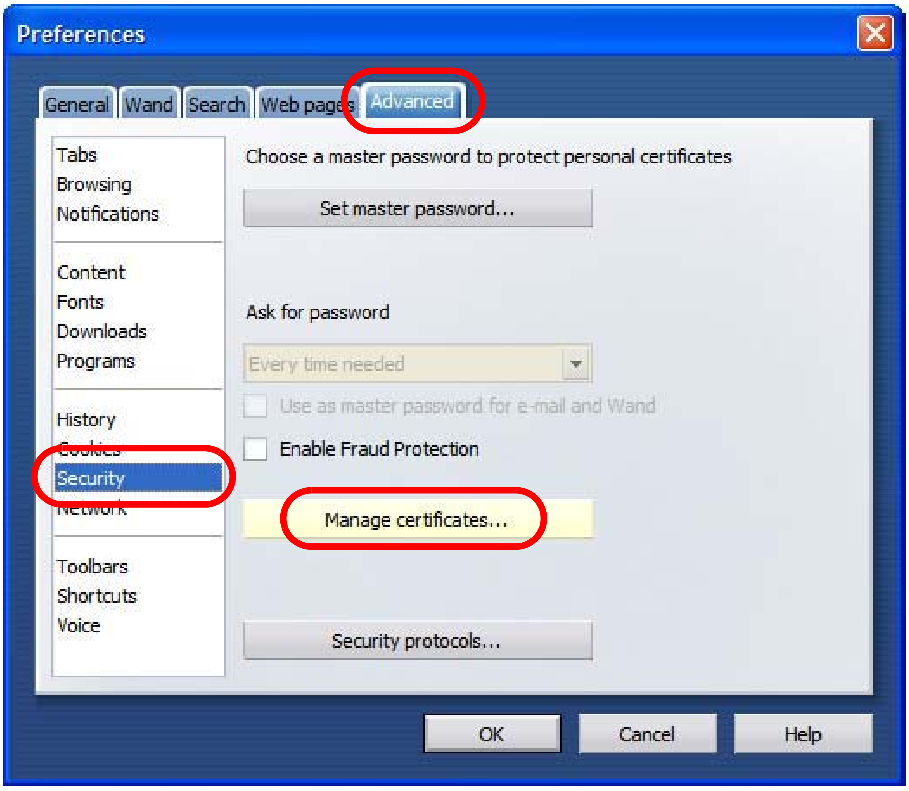
1 Open **Opera** and click **TOOLS > Preferences**.

Figure 219 Opera 9: Tools Menu



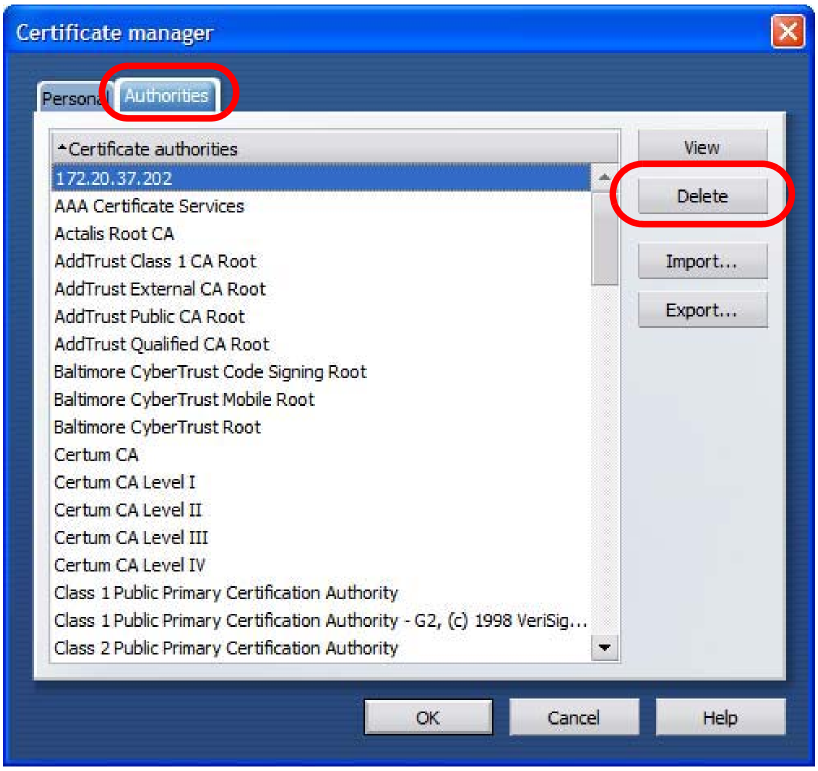
2 In **Preferences**, **ADVANCED > Security** > **Manage certificates**.

Figure 220 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 221 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.

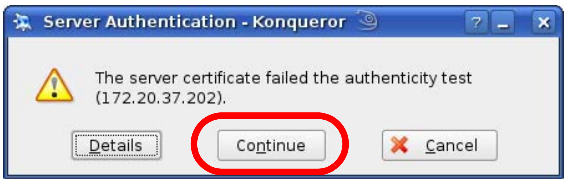
Konqueror

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 222 Konqueror 3.5: Server Authentication

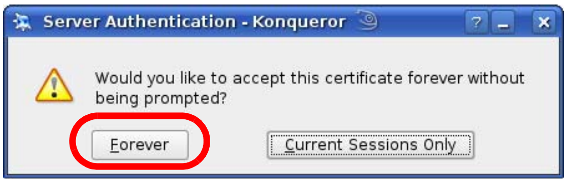


Server Authentication - Konqueror

The server certificate failed the authenticity test (172.20.37.202).

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

Figure 223 Konqueror 3.5: Server Authentication

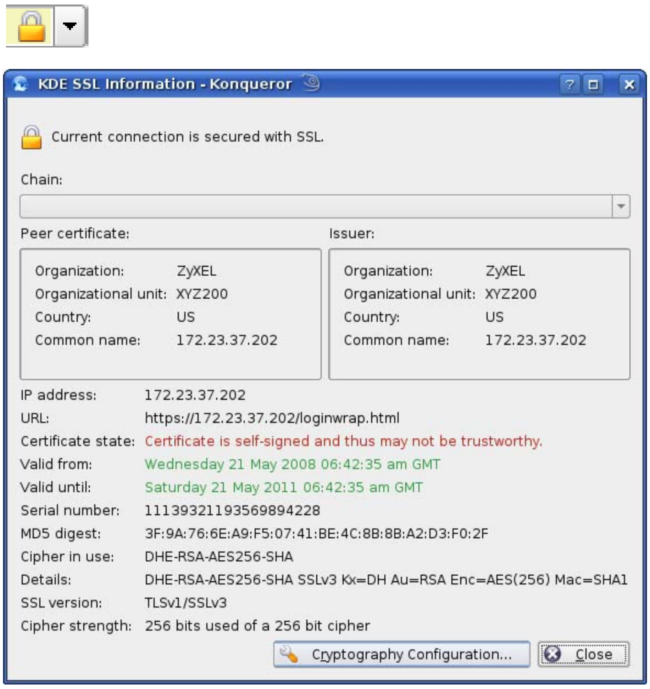


Server Authentication - Konqueror

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 224 Konqueror 3.5: KDE SSL Information



KDE SSL Information - Konqueror

Current connection is secured with SSL.

Chain:

Peer certificate:

Organization: ZyXEL
Organizational unit: XYZ200
Country: US
Common name: 172.23.37.202

Issuer:

Organization: ZyXEL
Organizational unit: XYZ200
Country: US
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

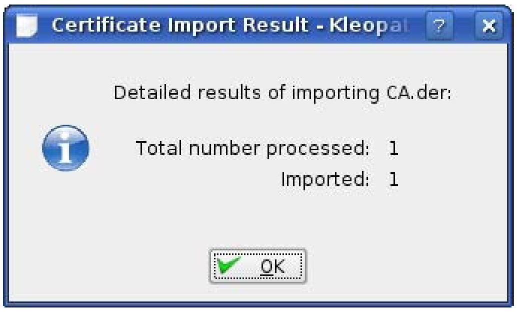
Rather than browsing to a Huawei web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 225 Konqueror 3.5: Public Key Certificate File

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

Figure 226 Konqueror 3.5: Certificate Import Result

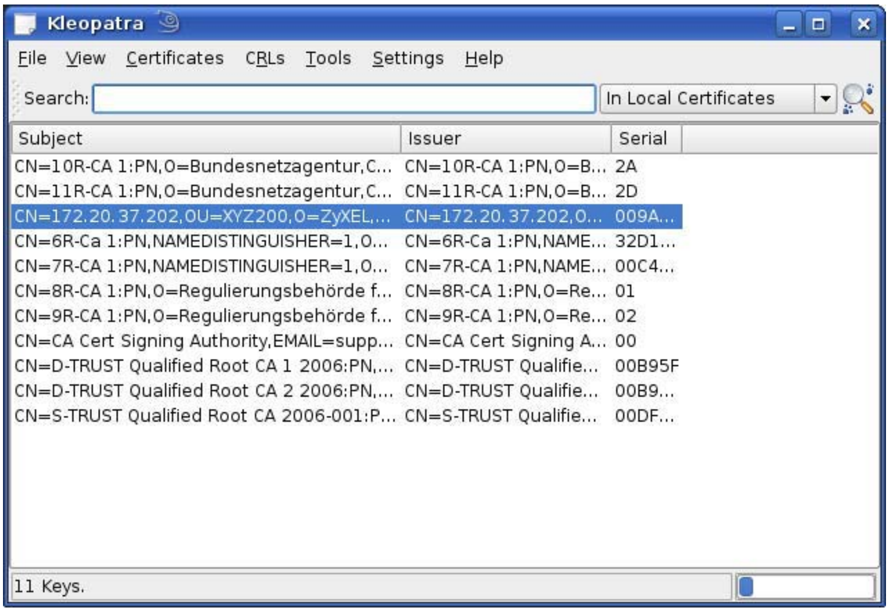


Detailed results of importing CA.der:

Total number processed: 1
Imported: 1

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

Figure 227 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.

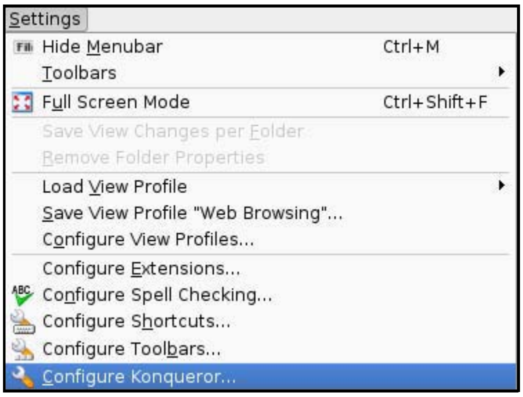
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

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**.

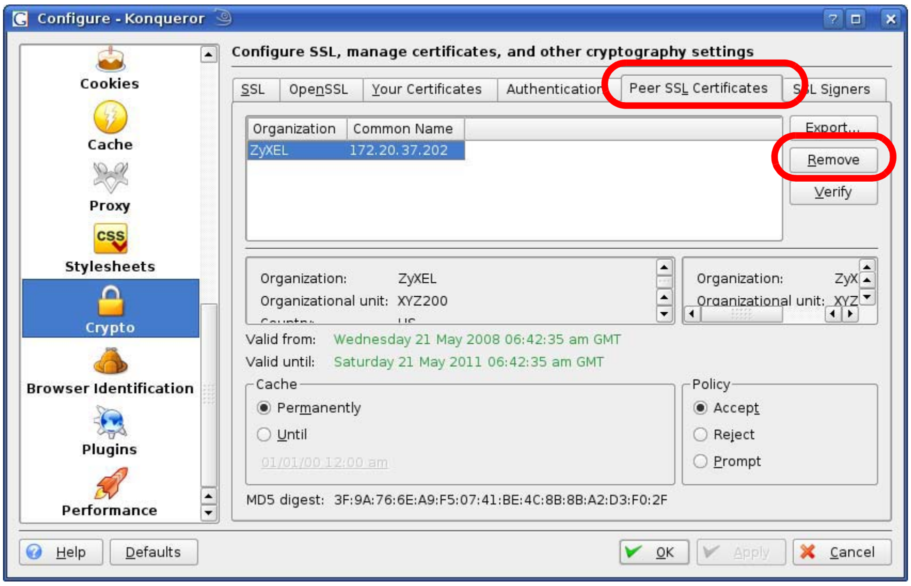
Figure 228 Konqueror 3.5: Settings Menu



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 229 Konqueror 3.5: Configure



Organization	Common Name
ZyXEL	172.20.37.202

Organization: ZyXEL
Organizational unit: XYZ200
Country: US

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.

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 121 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.Huawei.com) to IP numbers.
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.

Table 121 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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).
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.

Table 121 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

G

Legal Information

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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. (for all wireless devices)
- 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. (for all wireless devices without SAR test, such as an AP or wireless router. the SAR test will be done for wireless USB adapters and CardBus cards)

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 device is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l’ARCEP, la puissance d’émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d’une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

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.

Index